Jailson Eduardo Ramos Brito Évora

Desenvolvimento de um modelo de Política de Segurança da Informação em conformidade com a Gestão de Riscos:

Estudo do caso Uni Piaget CV

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

21.6.13

Jailson Eduardo Ramos Brito Évora

Desenvolvimento de um modelo de Política de Segurança da Informação em conformidade com a Gestão de Riscos:

Estudo do caso Uni Piaget CV

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

21.6.13

Jailson Eduardo Ramos Brito Évora , autor da monografia intitulada Desenvolvimento de um modelo de Política de Segurança da Informação em conformidade com a Gestão de Riscos, declaro que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia ao 21 de Junho de 2013
Jailson Eduardo Ramos Brito Évora

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Engenharia de Sistemas e Informática.

Sumário

Este trabalho foi realizado no âmbito do regulamento dos Cursos de Graduação da Universidade Jean Piaget de Cabo Verde, apresenta a concepção de um Modelo de Política de Segurança da Informação em conformidade com a Gestão de Riscos, evidenciado a importância que a mesma possui, como mecanismo de protecção da informação.

Apresenta assim um modelo desenvolvido na Universidade Jean Piaget de Cabo Verde a fim de preservar os recursos pertinentes da organização ao que se refere a segurança da informação, onde a partir de uma Avaliação/Análise de Risco efectuado previamente, desenvolveu-se um modelo de PSI que assegure a conformidade com a Gestão de Risco, sendo este (PSI) o ponto de partida no processo de implementação da segurança da informação.

Os objectivos traçados foram atingidos com sucesso sem grandes sobressaltos.

Palavras-chaves: Política de Segurança da Informação e Gestão de Riscos

Agradecimentos

À **Deus.**

Aos meus Pais.

Um especial agradecimento ao professor Jair Delgado pela, sua orientação, pela sua disponibilidade e pela sua motivação na realização deste trabalho monográfico.

Por último mas não menos importante, vai um especial agradecimento ao tutor Jairson Mendes.

Glossário

ABNT - Associação Brasileira de Normas Técnicas.

AS/NZS – Australian/New Zealand Standard ou padrão técnico Austrália/Nova Zelândia

Backup - cópia dos dados do computador de modo que possa ser usada para restaurar o original após um evento de perda de dados.

BS – British Standart – Padrão Britânico de Normas Técnicas.

DDOS - ***distribuídos ataque de negação de serviço*** é uma tentativa de fazer um recurso de máquina ou rede ficar indisponível para seus utilizadores.

DNS - ***D*omain *N*ame *S*ystem** sistema de gestão de nomes hierárquico e distribuído operando segundo duas definições: examinar e actualizar a base de dados; resolver nomes de domínios em endereços de rede (IP).

Firewall - baseado em software ou hardware é usado para ajudar a manter uma rede segura.

Força bruta - algoritmo trivial mas de uso muito geral que consiste em enumerar todos os possíveis candidatos de uma solução e verificar se cada um satisfaz o problema.

Gateway - ou ***ponte de ligação***, máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.

GR - *Gestão de Riscos de Segurança da Informação*

HB - Handbook Risk Management Guidelines Companion to AS/NZS 4360:2004 ou manual de Gestão de Riscos.

ISMS - ***Information Security Management System*** *ou Sistema de Gestão de Segurança da Informação.*

ISO/IEC - norma de segurança da informação publicada pela Organização Internacional de Normalização (ISO) e pela International Electro technical Commission (IEC).

IP - ***Internet Protocol*****-** sequência de números composta de 32 bits, que consiste em um conjunto de quatro sequências de 8 bits.

IT Governance Institute Cobit - Control Objectives for Information and related Technology

Ldap - ***Lightweight Directory Access Protocol***, protocolo para actualizar e pesquisar directórios sobre TCP/IP.

NBR – Norma Brasileira **abreviatura de** Associação Brasileira de Normas Técnicas.

P2P - arquitectura de sistemas distribuídos caracterizada pela descentralização das funções na rede, onde cada nodo realiza tanto funções de servidor quanto de cliente.

Port Scanner - aplicativo desenhado para "varrer" portas em host na rede.

PSI - *Política de Segurança da Informação.*

RFC 2196 - ***Request for Comments*** guia para a definição de políticas de segurança de computadores e procedimentos para sítios que possuem sistemas na Internet

Samba - servidor utilizado em sistemas operacionais do tipo Unix, que simula um servidor Windows, permitindo que seja feito a operações em rede Microsoft.

Servidor Pdc - ***Primary Domain Controller***, servidor em domínio do Windows, tem uma conta de administração, que tem total controlo dos recursos do domínio.

Servidor Proxy - servidor intermediário que atende a requisições transmitindo os dados do cliente.

Servidor www - servidor responsável por aceitar pedidos HTTP de clientes.

Sniffer - ***analisador de pacotes*** geralmente aplicativo que pode interceptar e registar o tráfego ao longo de uma rede ou parte de uma rede.

Spam - mensagem electrónica não-solicitada enviada em massa.

Vpn - ***virtual private network*** estende-se uma rede privada e os recursos contidos na rede através de redes públicas como a Internet.

Conteúdo

Glossário 7

Capítulo 1: Introdução 14
1.1 Contextualização 14
1.2 Relevância de estudo 15
1.3 Objectivos 16
1.4 Metodologia 16
1.5 Estrutura do trabalho 17

Capítulo 2: Conceitualização da Segurança da Informação 18
2.1 Classificação da Informação 19
2.1.1 Secreta 19
2.1.2 Confidencial 19
2.1.3 Interna 20
2.1.4 Públicas 20
2.2 Pilares de Sistema Seguro 20
2.2.1 Autenticidade 21
2.2.2 Confidencialidade 22
2.2.3 Integridade 22
2.2.4 Disponibilidade 23
2.3 Ameaças e Vulnerabilidades 24
2.4 Modelos de Controlo de Acesso e Mecanismo de Segurança 27

Capítulo 3: Gestão de Riscos 31
3.1 Conceito do risco 32
3.1.1 Equação do risco 33
3.2 Origem e classificação dos riscos 34
3.2.1 Riscos naturais 35
3.2.2 Riscos não intencionais 35
3.2.3 Riscos intencionais 36
3.3 Benefícios e factores críticos de sucesso para a gestão de risco 36
3.3.1 Factores críticos de sucesso 37
3.3.2 Benefícios 37
3.4 Etapas da avaliação de riscos 38
3.5 Prevenção vs. Reacção 43
3.6 Métodos de análise 43
3.6.1 Método quantitativo 44
3.6.2 Método qualitativo 46
3.7 Modelos de gestão de riscos 48
3.7.1 Modelo segundo a norma ISO Guide 73:2002 48
3.7.2 Modelo segundo a norma AS/NZS 4360:2004 49
3.7.3 Modelo segundo o IT Governance Institute (COBIT 4.1) 50
3.7.4 Modelo segundo a norma ISO 27005:2008 51
3.7.5 Modelo segundo a norma BS 7799-3:2006 52

Capítulo 4: Política de Segurança da Informação 54
4.1 Políticas de Segurança da Informação 55
4.2 Características de uma política 56
4.3 Importância de uma política de segurança 57

4.4 Tipos de políticas 59
4.5 Diagrama de conceito da Política de Segurança 60
4.6 Formulação de Política de Segurança da Informação 61
4.6.1 Finalidade 61
4.6.2 Conteúdo 61
4.6.3 Implementação 62
4.6.4 Revisão 63
4.7 Modelos de Segurança 64

Capítulo 5: Desenvolvimento de um modelo de PSI- o caso da Uni Piaget CV 66
5.1 Organização 67
5.1.1 Órgãos de governo da Universidade 68
5.1.2 Unidades Organizacionais 68
5.1.3 Infra-estruturas das Tecnologias de informação 69
5.2 Avaliação de Risco 69
5.2.1 Análise de Risco 70
5.2.1.1 Identificação de Riscos 70
5.2.1.2 Estimativa do Risco 79
5.2.2 Avaliar o Risco 82
5.3 Modelo de Politica de Segurança da Informação desenvolvido 82
5.3.1 Objectivos 83
5.3.2 A Informação 84
5.3.3 Princípios da Segurança da Informação 84
5.3.4 Política de Segurança da Informação 84
5.3.5 Políticas de Segurança Lógica 85
5.3.5.1 Administração de Contas 85
5.3.5.1.1 Caracterização geral 85
5.3.5.2 Autenticação 89
5.3.5.2.1 Política de palavra-passe 89
5.3.5.3 Correio-electrónico 90
5.3.5.3.1 Política de correio-electrónico 90
5.3.5.4 Acesso a Internet 91
5.3.5.4.1 Política de acesso a Internet 92
5.3.5.5 Utilização de Rede 93
5.3.5.5.1 Política de utilização de Redes (Wired) 93
5.3.5.5.2 Política de utilização de Redes (Wireless) 95
5.3.5.6 Estações de Trabalho 96
5.3.5.6.1 Política de utilização de estacão de Trabalho 96
5.3.5.7 Impressora 97
5.3.5.7.1 Política de utilização de Impressora 97
5.3.5.8 Backup 97
5.3.5.8.1 Política de backup 98
5.3.5.9 Vírus e Malware 99
5.3.5.9.1 Política de vírus e código malicioso 100
5.3.6 Políticas de Segurança Física 100
5.3.6.1 Controlo de acesso 100
5.3.6.1.1 Política de controlo de acesso 101
5.3.6.2 Mesa limpa e Bloqueio de ecrã (clear desk and lock screen) 101
5.3.6.2.1 Política de mesa limpa e bloqueio de ecrã 101
5.3.6.3 Utilização de laboratórios de informática 102
5.3.6.3.1 Política de utilização de laboratórios de informática 102

5.3.7 Âmbito Social 104
5.3.7.1 Continuidade dos negócios 104
5.3.7.1.1 Membros da Divisão Tecnológica 105
5.3.8 Termo de Concordância 105
5.3.9 Verificação da utilização da política 105
5.3.10 Violação da Política, advertência e punições 106

Conclusão 107

Bibliografia 112

Anexo 115
I. Lista de verificação 115
II. Guião de entrevista 120

Tabelas

Tabela 1: Matriz de riscos (V. A vs. N. A e V), adaptado (BS 7799-3:2006).....42
Tabela 2: Matriz de riscos (P vs. C), adaptado (HB 436:2004).....42
Tabela 3: Matriz de riscos (A, V e P), adaptado (HB 436:2004) 42
Tabela 4: Tabela de mapeamento qualitativo, adaptado (Wheeler, 2011) 47
Tabela 5: Determinação do risco qualitativo, adaptado (Landoll, 2011) 47
Tabela 6: ISMS ISO/IEC 27005:2008, adaptado (ISO/IEC 27005:2008).....52
Tabela 7: Recursos (Activos) Identificados.....71
Tabela 8: Vulnerabilidades RH/Organização e ameaças relacionadas.....74
Tabela 9: Vulnerabilidades Físicas e ameaças relacionadas 76
Tabela 10: Vulnerabilidades Lógicas e ameaças relacionadas.....78
Tabela 11: Escala de consequência, adaptado (AS/NZS 4360:2004 (HB 436:2004)) 79
Tabela 12: Escala de probabilidade, adaptado (AS/NZS 4360:2004 (HB 436:2004)).....79
Tabela 13: Matriz de Risco (P vs. I), adaptado (AS/NZS 4360:2004 (HB 436:2004)).....80
Tabela 14: Nível de Risco Identificados.....81
Tabela 15: Membros da Divisão Tecnológica, (DT 2013).....105

Figuras

Figura 1: Equação de risco, adaptado (Landoll, 2011)....33
Figura 2: Diagrama de Ishikawa, adaptado (Dantas, 2011) 40
Figura 3: Método OCTAVE, adaptado (Dantas, 2011)....41
Figura 5: Etapas de G.R. ISO/IEC Guide 73:2002, adaptado (ISO/IEC Guide 73:2002)....49
Figura 6: Etapas de G.R. AS/NZS 4360:2004, adaptado (AS/NZS 4360:2004)....50
Figura 7: Etapas G.R. BS 7799-3:2006, adaptado (BS 7799-3:2006)....53
Figura 8: Relação dos objectivos de PSI, adaptado (Wadlow, 2000)....58
Figura 9: Diagrama de conceito dos componentes da política, adaptado (Spanceski, 2004)...60
Figura 10: Modelo de Formulação de PSI, adaptado (Ferreira, 1995)....63

Capítulo 1: Introdução

1.1 Contextualização

As tecnologias de informação transformaram e de que maneira as estruturas organizacionais. Não podemos esquecer que além de trazer melhorias significativas, ela também trouxe consigo novas ameaças à integridade da informação. As ameaças intencionais e não intencionais colocam em risco a autenticidade, confidencialidade, integridade e disponibilidade da informação.

A 11 de Setembro de 2001 um ataque terrorista devastou um dos maiores centros económicos do mundo actual, em Dezembro de 2004, a fúria da natureza provocou uma das maiores catástrofes naturais, o Tsunami. Ambos tiveram consequências em comum, a perda do maior activo de uma organização, a informação. Varias instituições sediadas na World Trade Center, acabaram por fechar depois dos ataques, devido a inexistência de planeamento e medidas eficientes, capazes de colmatar as perdas relata Dantas (2011).

Ainda segundo Dantas (2011) ataques recentes a *sites* governamentais norte-americano demostraram a fraqueza de sistemas informáticos vulneráveis. Documentos confidenciais foram divulgados no *site* da Wikileaks. Actualmente uma das maiores empresas petrolíferas teve a sua segurança física violada, onde foram roubados computadores que continham informações confidências. Esta falha pôs em risco uma receita astronómica.

A segurança lógica, física e de recursos humanos deve ser levado muito a sério quando se fala da preservação da informação. As vulnerabilidades encontradas tanto na segurança lógica como na segurança física e de recursos humanos levaram a que seja possíveis tais acontecimentos ameaçarem os pilares de um sistema seguro.

Todas as organizações precisam elaborar políticas restritivas que assegure a conformidade com a gestão de risco para proteger as suas informações e garantir a segurança de toda a organização.

Actualmente as tecnologias de informação estão dotadas de mecanismos e procedimentos, que implementadas de maneira correcta e de acordo com o cenário, mitigará os riscos intencionais e não intencionais. Sabendo disso, elaborou-se algumas perguntas de partida, onde pretende-se até o final do referido estudo responder-se as mesmas.

Eis as seguintes perguntas de partida que se colocam na realização deste trabalho monográfico:

- Existem Políticas de Segurança da Informação adequadas e aprovados para a protecção da informação voltada para a segurança da informação?
- A gestão de riscos (tratamento de riscos) está previamente delineada em conformidade com as políticas de segurança da informação.

1.2 Relevância de estudo

Na era actual em que vivemos, era da informação, depara-se com uma questão pertinente. Como preservar um dos maiores activos de uma organização (a informação)?

A Segurança da Informação tem estado debaixo de varias ameaças, ameaças essas que colocam em risco a integridade da informação. Não esquecendo de que essas ameaças podem ser atenuadas e combatidas a partir da implementação de medidas de segurança tais como políticas de segurança da informação. Pretende-se a partir de uma Avaliação/Análise de Risco efectuado previamente desenvolver um modelo de PSI que assegure a conformidade com a GR, sendo uma PSI o ponto de partida no processo de implementação da segurança da informação.

1.3 Objectivos

Esta memória tem como objectivo geral:

- Desenvolver um modelo de Política de Segurança da Informação em conformidade com a Gestão de Riscos focada no ambiente organizacional da Universidade Jean Piaget,

O objectivo específico assenta:

- Em conhecer a importância de uma PSI como medida de prevenção e se a mesma está delineada em conformidade com a gestão de riscos (tratamento de risco);
- Em realizar uma Avaliação/Análise de risco a segurança da informação da instituição.
- E desenvolver um modelo de política de segurança da informação adequado a realidade da instituição, levando em conta a análise de riscos efectuado a priori.

1.4 Metodologia

A metodologia a ser adoptada neste trabalho enquadra na tipologia de estudo de caso onde a partir da descrição e interpretação de caso em estudo procura-se responder aos objectivos traçados, além da pesquisa documental e bibliográfica. A pesquisa de campo (estudo de caso), ou seja, o conhecimento na prática sobre gestão de riscos, implementação de políticas, vulnerabilidades, ameaça, riscos e formas de protecção.

A recolha de dados baseia-se, no primeiro momento, numa revisão da literatura onde serão abordados os conceitos teóricos que serviram para analisar os pontos chaves e fundamentais para compreensão do tema e a partir daqui formular o instrumento de colecta de dados.

No segundo momento, realiza-se uma pesquisa fundamentada nas técnicas de questionário e entrevista, na recolha de informações direccionado aos responsáveis da área de segurança da informação da instituição. Finaliza com uma Avaliação de Riscos e o desenvolvimento de um modelo de política de segurança da informação.

1.5 Estrutura do trabalho

O trabalho inicia-se pelo capítulo 1, Introdução, onde faz referência ao tema em estudo, a contextualização, a relevância do estudo, definição dos objectivos gerais e específicos, às hipóteses, às metodologias utilizada e por fim, breve explicação da estrutura do trabalho monográfico.

No segundo capítulo, inicia a contextualização teórica, ocupando-se da questão de conceitualização da segurança da informação, classificação da informação, pilares de um sistema seguro, ameaças, vulnerabilidades e por fim de mecanismo de segurança.

No terceiro capítulo, ocupa-se do tema Gestão de Riscos, definindo benefícios e factores críticos de sucesso, modelo de gestão de riscos, o processo de avaliação de riscos, identificação dos riscos, análise dos riscos à avaliação dos riscos.

No quarto capítulo, apresenta-se a temática da Política de Segurança da informação. Nesta perspectiva, aborda-se as características de uma política, importância de uma política, modelos de segurança, tipos de políticas, diagrama de conceito da PSI e formulação de PSI.

E por fim o quinto capítulo dedica-se à apresentação do estudo prático efectuado sobre o desenvolvimento de um modelo de política de segurança informação na Uni Piaget, onde caracteriza-se as suas estruturas organizações, as infra-estruturas das TIC’s, passando pela realização de uma Avaliação/Análise de risco, bem como os resultados chegados.

Por último apresenta-se as conclusões deste estudo sobre assuntos anteriormente levantadas na etapa introdutória. Como parte integrante deste trabalho monográfico, tende-se ainda a bibliografia de apoio, os apêndices para um melhor esclarecimento dos dados.

Capítulo 2: Conceitualização da Segurança da Informação

Sendo este o primeiro capítulo do estudo das artes, procura-se expor conhecimentos relacionados a segurança da informação.

Primeiramente apresenta-se as visões de vários autores referentes a classificação da informação, retratando a divisão que esta está sujeita, divisão essa que passa pela informação secreta, confidencial, interna ou pública.

É igualmente importante conhecer os pilares de sistema seguro, conceitos tais como, a autenticidade, a confidencialidade, a integridade e a disponibilidade da informação.

Ainda neste mesmo capítulo apresenta-se os conceitos de ameaças e vulnerabilidade, dando enfâse em ameaças e vulnerabilidades comuns, a partir da consulta efectuado a várias literaturas e normas de implementação da segurança da informação.

Finaliza-se o capítulo com os Modelos de Controlo de Acesso e Mecanismo de Segurança, onde apresenta-se a partir de serviços de segurança, uma série de mecanismo e controlos de acessos necessários para a implementação do processo de segurança.

2.1 Classificação da Informação

A importância da classificação da informação depara na necessidade que as organizações possuem para determinar o nível de protecção das suas informações, de maneira que a segurança seja resguarda.

> *"O objectivo da Classificação da Informação é assegurar que os activos da informação recebam um nível adequado de protecção. A informação deve ser classificada para indicar a importância, a prioridade e o nível de protecção. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de protecção ou tratamento especial. Um sistema de classificação da informação deve ser usado para definir um conjunto apropriado de níveis de protecção e determinar a necessidade de medidas especiais de tratamento"* segundo a descrição do item 5.2 da NBR ISO 17799", apud Spanceski (2004).

Actualmente a divisão da informação é feita em quatro níveis diferentes: secreta, confidencial, interna e pública, segundo Dias (2000) apud Spanceski (2004).

2.1.1 Secreta

Entende-se por informações secretas aquelas que uma vez divulgadas colocam em risco os negócios da organização, ou seja, informações críticas cujo acesso deve ser restrito a um número reduzido de pessoas e deve ser preservada a sua integridade.

Segundo Spanceski (2004) o acesso interno ou externo por pessoas não autorizadas a esse tipo de informação é extremamente crítico para a instituição.

2.1.2 Confidencial

As informações confidenciais devem ser disseminadas somente para indivíduos previamente definidos. A sua divulgação pode levar a perdas financeiras, instabilidade operacional da organização até a perda da confiabilidade perante os clientes na perspectiva de Laureano (2005).

O acesso não autorizado há estas informações podem causar danos financeiros ou perdas de fatia de mercado para o concorrente entende Spanceski (2004).

2.1.3 Interna

Segundo Laureano (2005) essas informações só devem ser divulgadas dentro das empresas. Apesar do seu conteúdo não ser vital para a organização, é pertinente preservar a sua integridade.

2.1.4 Públicas

Laureano (2005) define como sendo divulgadas dentro e fora das empresas, sem consequências danosa e cuja integridade não é vital para a informação.

Por sua vez Spanceski (2004) entende que podem ser divulgadas para o público em geral, incluindo clientes, fornecedores, imprensa, e não possuem restrições para divulgação.

2.2 Pilares de Sistema Seguro

Segundo o modelo original um sistema seguro deve garantir para a informação, três características fundamentais: a confidencialidade, a integridade e a disponibilidade. Esses devem ser preservados, pois são os pilares de sistemas seguro.

> *"Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas."* (NBR ISO/IEC 27002:2005) apud Dantas (2011).

Apesar do modelo original ser CID, isto não significa a inexistência de outros modelos. Segundo a norma ABNT NBR ISO/IEC 27002:2005 adicionalmente, outras propriedades, tais como autenticidade e responsabilidade.

A segurança da informação segundo a norma ABNT NBR ISO/IEC 27002:2005 apud Dantas (2011) assenta na protecção da informação contra vários tipos de ameaças e riscos de forma a garantir a continuidade e maximizar os lucros do negócio.

Por sua vez Sêmola (2003) apud Freitas (2009) define a segurança da informação como ciência dedicado a protecção de activos da informação contra intrusos, a falta de autenticidade ou sua indisponibilidade.

Wheeler (2011) entende que:

> "*The goal of Information Security must be to ensure the confidentiality, integrity, availability, and accountability of the resources for which we are responsible. The desirable level of assurance varies between organizations, between industries, and may be even between departments within the same organization."*

Wheeler (2011) afirma que os três pilares fundamentais da segurança da informação são comummente conhecidas como confidencialidade, integridade e disponibilidade, acrescenta que a segurança evoluiu e que há necessidade de acrescentar mais uma característica aos pilares de sistemas seguro, a responsabilidade.

Ele define a responsabilidade como "*Accountability describes the need for the ability to trace activities to a responsible source."* Wheeler (2011).

2.2.1 Autenticidade

Spanceski (2004) define a como a medida de protecção de um serviço/informação contra a personificação por intrusos."

Quando referimos a autenticidade, logo associamos a identificação do utilizador. A autenticidade pode ser definida como sendo a protecção de informação e serviços contra a personificação por indivíduos não autorizados.

O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo, relata Spanceski (2004).

O objectivo principal assenta no reconhecimento e evitar personificação, assegurar que quem diz ser é realmente a correcta. A informação é de quem a assinou.

2.2.2 Confidencialidade

É mesmo que proteger a informação ou serviço contra o acesso a intrusos. A confidencialidade da informação é quebrada quando o seu conteúdo for acessado por pessoas não autorizados. Garantir a confidencialidade requer evitar a divulgação não autorizada da informação e assegurando o valor da mesma.

Segundo a norma ABNT NBR ISO/IEC 27002:2005 apud Dantas (2011), a confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

"A informação somente pode ser acessado por pessoas explicitamente autorizadas; É a protecção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo" Laureano (2005).

Wheeler (2011) entende que a confidencialidade da informação deve ser garantida na medida que elas não devem ser divulgadas a pessoas não autorizadas, processos e dispositivos.

Segundo Mamede (2006) a confidencialidade tem a ver com o estabelecimento de segredo, assegurando que algo ou alguém não tem autorização.

2.2.3 Integridade

A integridade assenta na protecção da informação ou serviço contra a modificação/ danos por indivíduos não autorizados e tem por objectivos evitar e detectar alterações nas informações.

A quebra da integridade acontece quando a informação é falsificada, destruída, roubada ou corrompida.

A informação deve manter no seu estado original. Impedir que ela seja criada, modificada ou destruída na perspectiva de Wheeler (2011).

"A integridade é a garantia da exactidão e informação completa dos métodos de processamento ABNT NBR ISO/IEC 27002:2005 " apud Dantas (2011).

Laureano (2005) por sua vez define-a como a protecção da informação contra modificações intencionais ou acidentes não-autorizadas.

Mamede (2006) relaciona a integridade à garantia de que tudo está como deve estar e assim se mantém ao longo do tempo. A integridade é também um sinónimo para consciência externa.

2.2.4 Disponibilidade

A disponibilidade é a garantia de que os utilizadores autorizados obtenham acesso à informação e aos activos correspondentes sempre que necessário, referenciado pela norma ABNT NBR ISO/IEC 27002:2005 apud Dantas (2011).

Manter a disponibilidade requer o repúdio de acções que visem a rejeição de acesso a determinados serviços ou informação em tempo útil.

Wheeler (2011) define-a como em caso de necessidade, ela seja acessado em tempo útil, confiável por utilizadores autorizados.

A disponibilidade pode estar comprometida quando a informação não esta disponível para acesso em tempo útil a ser utilizada por utilizadores e destinatários, ou seja a informação não circula.

A disponibilidade responsabiliza-se por garantir que os recursos estão disponíveis na altura em que são necessários entende Mamede (2006).

Garantir a disponibilidade requer o êxito no carregamento, transporte e armazenamento da informação.

2.3 Ameaças e Vulnerabilidades

Podemos definir a ameaça como sendo um evento com um impacto indesejado que pode resultar na perda, dano, divulgação de um activo organizacional.

Landoll (2011) define uma lista parcial de ameaças:

- **Erros e Omissões** - erros por funcionários autorizados, utilizadores, desenvolvedores e profissional de teste que podem levar a falta de dados e de integridade do sistema e mesmo a divulgação de informações confidenciais.
- **Fraude e Roubo-** acto de fraudar activos institucionais pondo em causa as características de um sistema seguro.
- **Sabotagem-** funcionários autorizados podem utilizar a confiança depositada para sabotar a instituição, pode incluir dano físico, destruição de processos, exclusão de dados ou perda de integridade de dados.
- **Perda do suporte físico e da infra-estrutura-** ameaça de varias origem que incluem falhas de energia, tempestades de inverno, greves, e ataques terroristas.
- **Espionagem-** acto de adquirir/roubar dados alheios para o propósito de ajudar outra organização. Espionagem é realizada por governos estrangeiros e organizações competitivas.
- **Código Malicioso-** aplicativos maliciosos pode ser um vírus, cavalos de Tróia, Worms, bombas lógicas.
- **Divulgação-** perda de confidencialidade da informação.

Um agente de ameaça é a entidade que pode causar uma ameaça acontecer. Ameaças e agentes de ameaça estão intimamente ligadas, na medida em que é o agente de ameaça que causa o acontecimento de uma ameaça na perspectiva de Landoll (2011).

Segundo Landoll (2011) Agentes de ameaça são o catalisador da ameaça. Ele apresenta uma lista de agentes de ameaças:

- **Natural-** tempestades ou inundações, terramoto, etc. Landoll (2011) entende que então a "natureza" pode ser considerado o agente de ameaça.

- **Empregados-** um empregado pode cometer um erro crítico, pode de forma intencional ou não divulgar dados proprietários, ou até decidir em fraudar a organização.
- **Black Hackers-** apesar de não estar conectada a internet os activos da instituição podem estar sob ameaças, a partir de ataques de engenharia social entre outros tipos de ataques *off-line* perpetuado por *hackers.*
- **Industrial Spies-** a espionagem industrial pode resultar em perda de lucros, vantagem competitiva entre outros.
- **Foreign Government Spies-** governos estrangeiros utilizam da espionagem para conseguir avançar as suas habilidades ou até mesmo restringir o desenvolvimento do outro governo espionado.

Segundo Wheeler (2011), quando se fala na segurança dos dados, devemos pensar no controlo de três estados da informação:

- **Em Trânsito-** refere aos dados que estão a ser transmitidos electronicamente entre sistemas ou em transporte físico.
- **No Processo-** refere-se a protecção dos dados, como esta a ser usada pelo sistema ou aplicação.
- **Em Repouso-** foca-se na protecção dos dados no local do armazenamento. Tipicamente o controle para este estado inclui, Controlo de Acesso, Criptografia e a Protecção Física.

No entender de Wheeler (2011) cada estado que os dados possam tomar, há uma lista de ameaças a informação.

Descrevendo-os em quatro categorias principais sendo que os três primeiros mapeiam em Confidencialidade, Integridade e Disponibilidade e a quarta pertencente a Responsabilidade.

- **Divulgação não autorizada**, como uma violação de dados;
- **Corrupção**, tais como uma modificação acidental de um registo de dados;
- **Negação de serviço**, tal como um ataque que faz com que uma indisponibilidade de recurso;

- **Disponível para provar a Origem de um Ataque**, tais como o uso de uma conta partilhada para realizar uma actividade não autorizada.

Wheeler (2011) define ameaças no contexto da segurança da informação como sendo a fonte dos ataques e também a actividade ou meios do ataque.

Normalmente considera a fonte de ameaças o potencial de prejudicar o recurso, enquanto que, a actividade no seu entender, é a maneira pela qual vai ser prejudicado.

Ainda segundo Wheeler (2011) qualquer ameaça a segurança da informação enquadra numa dessas categorias:

- Desastre Natural
- Falta de Infra-estrutura
- Abuso Interno
- Acidente
- Ataque com alvo externo
- Ataque externo em massa

Vulnerabilidades

"As vulnerabilidades são pontos em que o sistema é susceptível a ataques" Freitas (2009).

Entende-se por vulnerabilidade como sendo o estado de um componente que compromete a segurança de todo o sistema, uma vulnerabilidade existe sempre enquanto não for corrigida. Existem vulnerabilidades que são intrínsecas ao sistema.

Não existem ataques bem-sucedidos sem a existência de um sistema vulnerável. Uma vulnerabilidade pode ser uma simples fraqueza ou uma série de pontos fracos que acabam permitindo uma ou várias ameaças.

No entender de Landoll (2011) a vulnerabilidade é uma falha num controle existente, que pode, eventualmente, permitir que um agente de ameaça possa explorá-lo para ganhar acesso não autorizado aos activos organizacionais.

"A vulnerabilidade é o ponto onde qualquer sistema é susceptível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc." Laureano (2005).

Para Sêmola (2003) apud Dantas (2011), as vulnerabilidades são fragilidades presentes ou associadas a activos de informação, que, ao serem exploradas, permitem a ocorrência de incidente na segurança da informação.

Landoll (2011) defende a existência de três conceitos chaves de vulnerabilidade, a vulnerabilidade administrativa, a vulnerabilidade técnica e a vulnerabilidade física. A vulnerabilidade administrativa consiste em lacunas nas políticas de segurança, nos procedimentos ou actividades de segurança.

Ele também define a vulnerabilidade técnica como sendo falhas nos controles lógicos, ou seja nos *softwares* mal configurados, portas em sistemas abertos sem utilidade.

Por sua vez também fala a respeito da vulnerabilidade física, considerando-os como sendo falhas nos sistemas da infra-estrutura física da organização, por exemplo buracos na cerca de vedação.

2.4 Modelos de Controlo de Acesso e Mecanismo de Segurança

Na perspectiva de Wheeler (2011) existem quatro modelos de controlo de acesso utilizados nos mais variados ambientes.

Controle de Acesso Discricionário- o acesso é controlado pelo proprietário onde restringe o acesso a recursos a partir da identidade e necessidade de saber a respeito de utilizadores ou grupos. Utilizado em grande escala nas comunicações usando o protocolo P2P.

Controle de Acesso Baseados na Função- baseado nas actividades dos utilizadores. Utiliza funções (responsabilidades) de trabalho, para definir o acesso ao recurso.

"Podemos restringir o acesso a escrita de dados para um determinado utilizador, deixando apenas o acesso a leitura, caso a sua actividade não tiver privilegio para tal (não possui actividades como a actualização, editar.) " Wheeler (2011).

Este controle é utilizado normalmente em sistemas de aplicação, onde cada responsabilidade é concedida acesso a privilégios e dados específicos.

Controle de Acesso Baseado em Regras- o acesso ao recurso é controlado a partir regras previamente definidas. Utilizados em dispositivos tais como, *firewall* ou *routers*.

Controle de Acesso Baseado no Conteúdo- pode ser entendido como a expansão do controle baseado em regras. O acesso também é controlado a partir da filtragem em protocolos de comunicações.

Wheeler (2011) relata que o fluxo de comunicações pode ajudar a prevenir ataques comuns, usando técnicas de disfarçar ou abusar de ambiguidade em protocolos padrão, mas isso também pode adicionar mais sobrecarga e latência para funções de inspecção.

Mecanismos de controlo de segurança

Segundo Laureano (2005) os mecanismos de controlo de segurança são:

- Autenticação e autorização
- Combate a ataques e invasões
- *Firewall*
- Detector de Intrusos

Por sua vez Wheeler (2011) tem uma visão mais alargada definindo a partir de serviços de segurança uma série de mecanismo:

- **Inspecção da comunicação-** canais encriptados também passam pela inspecção, mas técnicas como a estenografia são utilizadas para driblar esse mecanismo.
- **Validação da comunicação-** comunicações fora do padrão serão rejeitadas, pode-se abrir excepções desde de que se saiba a origem.
- **Filtragem da comunicação-** este fornece o mecanismo de distinção entre a informação autorizada e a não autorizada.
- **Aplicações de políticas-** as políticas podem ser implementadas em algumas áreas da segurança da informação.
- **Gestão de sessão -** sessão permite que aplicações mantenham estados. Ataques como roubo de sessão podem comprometer a integridade.

  Wheeler (2011) define alguns princípios da Gestão de Sessão que devem ser de execução universal, embora alguns detalhes podem variar:

  - ✓ **Controlo de sessão Simultânea -** sistema de informação limita o número de sessão simultâneo para qualquer utilizador.
  - ✓ **Bloqueio de sessão -** previne mais acessos aos sistemas, inicia o bloqueio de sessão depois do período de sessão inactivo, que permanece até que o utilizador reestabeleça o acesso. O bloqueio permanente pode ser utilizado para realizar ataques DOS contra o sistema.
  - ✓ **Enceramento de sessão -** o sistema automaticamente termina uma sessão local ou remoto, depois de um período de inactividade ou o tempo máximo de duração é excedido.
- **Autenticação-** validação da identidade de um individuo ou sistemas com o propósito de proteger os dados contra o acesso não autorizado e estabelecendo a responsabilidade.
- **Autorização-** a autorização define os tipos de acessos permitidos e quais os recursos que o acesso deve ser aplicada.
- **Auditoria/ Registo-** captação de eventos significativos em um sistema, em um aplicativo, ou em uma rede.

- **Criptografia-** a criptografia fornece muitas ferramentas essenciais para o exercício de controlos de segurança que preservam a integridade, responsabilidade, e confidencialidade dos dados.
- **Resiliência-** resiliência pode ser implementada em vários níveis, a partir de sistemas operacionais para aplicações e da infra-estrutura de rede para a infra-estrutura física que o suporta.
  - ✓ **Físico-** as fontes de alimentação e outros componentes físicos de sistemas devem proporcionar um certo nível de redundância integrada no dispositivo.
  - ✓ **Lógico-** podemos considerar que de certa forma, é impossível projectar um sistema que é impermeável a (DDoS). Tanto faz o poder da máquina, há sempre uma maneira de gerar tráfego suficiente para dominar os recursos.
- **Monitorização de eventos-** entradas notáveis irá apontar para a actividade anormal ou não autorizados que podem indicar uma violação de segurança.

  Wheeler (2011) demostra alguns dos importantes requisitos para o monitorização de eventos:
  - ✓ As entradas de log devem ser normalizadas em um formato comum
  - ✓ Serviços de monitorização de eventos devem responder por diferenças de fusos horários
  - ✓ Os registos devem ser correlacionados entre sistemas de origem e localizações
  - ✓ Deve incluir o monitorização em tempo real e alerta significativa
- **Gestão de vulnerabilidades-** monitorização de serviços em tempo real do entorno para as vulnerabilidades emergentes e também executar regularmente avaliações profundas.

  Wheeler (2011) entende qua a verificação inclui:
  - ✓ Níveis de patch
  - ✓ Serviços não autorizados ou vulneráveis
  - ✓ *Software* não autorizado ou vulnerável
  - ✓ Configurações não autorizadas ou vulneráveis
  - ✓ Controles de segurança insuficiente ou fracos
  - ✓ Credenciais de autenticação fraca e Protocolos vulneráveis

Capítulo 3: Gestão de Riscos

Sendo este um capítulo direccionado a gestão de riscos, pretende-se percorrer todos os conceitos chaves relacionado a mesma.

Primeiramente o capítulo inicia-se com o conceito do risco, ou seja a definição do risco, onde apresenta-se a equação do risco e suas variáveis.

Depois de entender o conceito de riscos, segue-se a origem dos riscos e suas classificações, tais como os riscos naturais, os não intencionais e os intencionais. Também são retratados factores que podem levar a estes acontecimentos, medidas que devem ser tomadas para mitigar esses riscos.

A necessidade de atingir os objectivos no processo de gestão dos riscos, torna-se necessário identificar os seus factores críticos de sucesso. Sendo verdade, pretende-se demostrar os factores que influenciam na realização de uma gestão de riscos adequado a realidade da instituição.

É igualmente importante antes de efectuar uma GR, conhecer as etapas da avaliação de riscos. Retrata-se as fases básicas de análise/avaliação de riscos independentemente do modelo escolhido, fases essas que incluem: a identificação dos riscos, a análise dos riscos e a

avaliação dos riscos. Apesar de não ter dado enfâse as restantes etapas do processo de GR, tais como o tratamento de risco, aceitação, a comunicação do risco e a monitorização, por não considerar-se como fundamentais para a realização do caso pratico. Mas mesmo assim, pode-se consultar essas fazes na parte Modelos de GR, já de uma forma menos aprofundada.

Não esquecendo a prevenção e a reacção, o actual capítulo engloba-as, onde pretende-se compreender as duas situações que uma análise de risco esta sujeita: a antecipação de eventos e a outra durante e após a ocorrência dos eventos.

Caminhando para o final do capítulo, é de grande importância retratar os métodos utilizados na avaliação dos riscos, métodos que englobam o quantitativo e o qualitativo. Métodos destintos de avaliar os recursos no processo de avaliação de risco, sendo cada uma com sua importância.

A Finalizar o capítulo, é importante realçar os modelos essências utilizados no processo de gestão de riscos. Segundo diversas normas, tais como, a ISO/IEC, a AS/NZS, o IT *Governance Institute*, passando pelo *British Standard*, todas elas com modelos específicos.

3.1 Conceito do risco

Dantas (2011) define o risco como sendo algo que cria oportunidades ou produz riscos. Em relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas.

Vários conceitos e definições podem ser encontrados para a definição dos riscos.

A norma AS/NZS 4360:2004 define risco como a *chance* de acontecer algo que vai ter um impacto sobre os objectivos, considerando que os riscos podem ter impacto negativo ou positivo.

Por sua vez Wheeler (2011) define o risco aplicado a segurança da informação, como sendo a expectativa da perda da confidencialidade, integridade, disponibilidade e responsabilidade da informação.

Ainda segundo Jack Jones apud Wheeler (2011), a definição do risco pode ser ainda entendido como sendo a probabilidade de ocorrência e magnitude de futuras perdas.

A partir destas duas definições Wheeler (2011) define o foco pretendido para a função da segurança da informação: "*The probable frequency and probable magnitude of future loss of confidentiality, integrity, availability, or accountability".*

A partir das definições dos diversos autores acima citados, conclui-se que o risco esta intimamente associado a probabilidade de ocorrência dum evento e suas consequências negativas.

3.1.1 Equação do risco

A determinação de risco de segurança, portanto, é dependente das ameaças identificadas medidas e vulnerabilidades, e baseado na probabilidade de ameaça/vulnerabilidade, o valor do activo afectado, e do impacto que ameaça / vulnerabilidade terá sobre o activo segundo Landoll (2011).

Na perspectiva de Landoll (2011) a equação básica para calcular o risco é:

Risco = Activos × Ameaças × Vulnerabilidade

Landoll (2011) entende que esta simples equação é uma mera ilustração do princípio do cálculo do risco baseado no conhecimento do valor do activo, estendido a ameaças e a probabilidade de ameaças explorar uma vulnerabilidade existente.

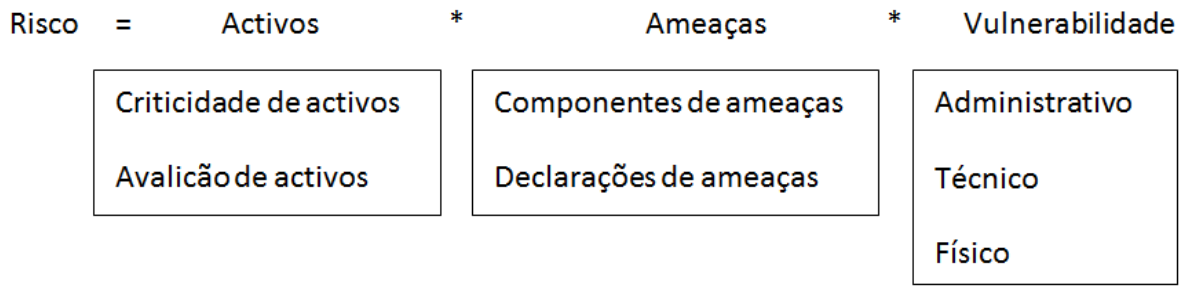

Figura 1: Equação de risco, adaptado (Landoll, 2011)

Por outro lado *Casada et al* (2003) apud Dantas (2011) apresenta uma equação diferente para o risco, representando-o como o produto da frequência (quantidade de eventos em determinado período) pela consequência ou impacto do evento.

(R) Risco = (C) Consequência * (P) Frequência

Ainda segundo Dantas (2011) para o cálculo baseado na combinação de eventos externos utiliza-se a combinação da ameaça com a vulnerabilidade, podendo vir a ser representado por:

P = T x V, em que: T= ameaça; e V= vulnerabilidade

Um outro autor tem uma equação diferente para o cálculo do risco, Sêmola (2003) apud Dantas (2011) apresenta a seguinte equação para o risco, diferenciando-se por acrescentar as medidas de segurança, que, segundo ele, devem ser consideradas na aferição do risco:

(R) risco= ((V) vulnerabilidade x (**A) ameaça** x (**I) impacto) / (M) medidas de segurança.**

[a]*Apesar das mais diversas equações possíveis para calcular o risco, o importante é compreende-lo na sua forma alargada, transpondo a clareza aos elementos vitais que influenciam na identificação, para uma melhor análise*[a] Dantas (2011).

Para além deste ponto, é também de importância, a probabilidade de identificar a sua origem tornando possível a sua classificação em categorias.

3.2 Origem e classificação dos riscos

Dantas (2011) entende que o risco pode ter várias origens, pode ser oriundo de eventos da natureza, pode ser decorrente de problemas técnicos, bem como ser o resultado de uma acção intencional.

Desta forma Dantas (2011) classifica os riscos em três categorias destintas, os riscos classificados como **naturais** são aqueles oriundos de fenómenos da natureza; os **involuntários** resultam de acções não intencionais, relacionados com vulnerabilidades humanas, físicas, de

hardware, de *software* entre outros, e os **intencionais** são aqueles derivados de acções deliberadas para causarem danos.

3.2.1 Riscos naturais

Segundo Dantas (2011) alguns factores devem ser considerados em relação aos riscos naturais:

- A área em que a empresa está instalada é sujeita a eventos da natureza, constantes ou não, de proporções catastróficas ou não;
- Falta de acompanhamento de boletins meteorológicos;
- Material empregado na construção de baixa resistência e/ou qualidade.
- Equipamentos de prevenção a sinistros (de origem na natureza) sem inspecção periódica e de má qualidade;
- Ausência de plano de recuperação de desastres e de continuidade dos negócios;
- Falta de treinamento em acções contingenciais.

Landoll (2011) entende que a determinação de riscos de segurança física para a construção de uma organização inclui uma análise dos riscos naturais e humanos.

3.2.2 Riscos não intencionais

Dantas (2011) afirma que, a identificação da sua origem tem relação directa com as vulnerabilidades humanas, físicas, de *hardware*, de *software*.

Ainda segundo Dantas (2011), alguns factores devem ser considerados em relação aos riscos involuntários, tais como:

- Falha nos equipamentos de prevenção e detecção;
- Descuido no cumprimento de normas para guarda, transporte e manuseio de material inflamável;
- Material de fácil combustão empregado na construção;

- Equipamentos ligados 24 horas;
- Ausência de treinamento em medidas contingenciais;
- Inexistência de processos de qualidade;
- Inexistência de controlos internos;
- Inexistência de programa de capacitação continuada;
- Cultura organizacional.

3.2.3 Riscos intencionais

Dantas (2011) descreve alguns factores que devem ser considerados em relação aos riscos intencionais, tais como:

- Situação do sistema de controlo interna;
- Atractividade do produto e sua fácil receptação no mercado paralelo;
- Área em que a empresa está instalada sujeita a eventos da natureza de proporções catastróficas;
- Situação da criminalidade na região em que a empresa está instalada;
- Sensação de impunidade;
- Pagamento efectuado, em espécie, aos funcionários da empresa;
- Funcionários insatisfeitos com salários em atraso e sem perspectiva de continuidade no emprego;
- Mercado altamente competitivo;
- Informações de alto poder estratégico.

3.3 Benefícios e factores críticos de sucesso para a gestão de risco

Na perspectiva de Dantas (2011), atingir os objectivos, torna-se necessário identificar as principais variáveis que influenciam directamente no seu desempenho, ou seja, os seus factores críticos de sucesso.

3.3.1 Factores críticos de sucesso

Dantas (2011) identifica os principais factores de sucesso para a gestão de riscos:

- O patrocínio da direcção da organização;
- A definição dos requisitos da gestão, alinhado com a missão e os objectivos da empresa;
- O estabelecimento do escopo de todo o processo;
- O ambiente das actividades de negócios e a criticidade do produto;
- A definição de uma equipa multidisciplinar para o macroprocesso e suas responsabilidades definidas;
- A definição dos colaboradores de diversas áreas da organização e as suas atribuições no processo;
- A forma da comunicação interna;
- A cultura da segurança da informação;
- A identificação dos principais activos e processos de negócios;
- A confiabilidade da lista das principais ameaças à segurança da informação;
- A escolha e a utilização do método de análise dos riscos;
- Os critérios de parâmetro para a classificação dos riscos e as medidas de tratamento;
- A implementação das medidas para o tratamento dos riscos;
- O controlo e a monitorização constante do processo.

3.3.2 Benefícios

A norma (HB 436:2004) associada a (AS/NZS 4360:2004) entende que os princípios fundamentais da gestão de risco são de natureza genérica e em grande parte independente de qualquer tipo individual de estrutura organizacional, apresentando os seguintes benefícios da gestão de riscos:

- Poucas surpresas;
- Exploração de oportunidades;

- Melhora o planeamento, desempenho, e eficácia;
- Economia e eficiência;
- Melhora o relacionamento com *stakeholder*;
- Melhora informação para a tomada de decisão;
- Melhora a reputação;
- Protecção dos directores;
- Responsabilidade, garantia e governação;
- Bem-estar pessoal.

3.4 Etapas da avaliação de riscos

As etapas da avaliação de riscos variam de acordo com o modelo escolhido. As normas ISO/IEC Guide 73 e BSI 7799-3:2005 estabelecem duas etapas para a avaliação de riscos: a análise do risco e a avaliação do risco (*risk evaluation*).

Já a norma AS/NZS 4360:2004 apresenta 3 etapas para a avaliação de riscos: identificar os riscos, analisar os riscos e avaliar os riscos (*risk evaluate*).

A escolha de um método de avaliação é um dos requisitos exigidos pela norma ISO 27001:2005, para se estabelecer um sistema de gestão da segurança da informação.

Segundo Dantas (2011), independentemente da escolha do modelo, 3 fases destacam-se durante a avaliação de riscos:

- Identificar os riscos;
- Analisar os riscos;
- Avaliar os riscos.

Identificar os riscos

As actividades são direccionadas para identificar onde, quando, o porquê e como os eventos podem ocorrer de forma a prejudicar as actividades de negócio da organização.

A norma ISO 27001:2005 estabelece que, ao identificar os riscos, a organização deve:

1) Identificar os activos dentro do escopo do ISMS e os proprietários desses activos;
2) Identificar as ameaças a esses activos;
3) Identificar as vulnerabilidades que podem ser exploradas pelas ameaças;
4) Identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos activos.

Identificar os activos e seus proprietários

Dantas (2011) afirma que nesta fase resulta em levantamento de todos os activos do ISMS, seus proprietários e um valor atribuído para cada activo que expresse a sua importância em relação à perda do requisito de segurança estabelecido.

"A identificação dos activos por si só não é suficiente, pois se torna necessário atribuir-lhe um valor de importância que ele representa para a organização em relação aos possíveis danos de um evento indesejável" Dantas (2011).

Identificar as ameaças aos activos

De maneira geral, as ameaças são tidas como agentes ou condições que exploram as vulnerabilidades e provocam danos segundo Dantas (2011).

Segundo Dantas (2011) uma técnica que pode ser utilizada para facilitar a identificação das ameaças é considerar a actividade de negócio e fazer as seguintes indagações: "o quê?", "quando?", "onde?" e "qual o agente motivador? ".

Identificar as vulnerabilidades

Dantas (2011) entende que uma técnica utilizada para a identificação de vulnerabilidades é o emprego do diagrama de causa e efeito.

Esse diagrama também é conhecido pela denominação de **diagrama de Ishikawa**, porque foi desenvolvido por Kaoro Ishikawa, em 1943, na Universidade de Tóquio.

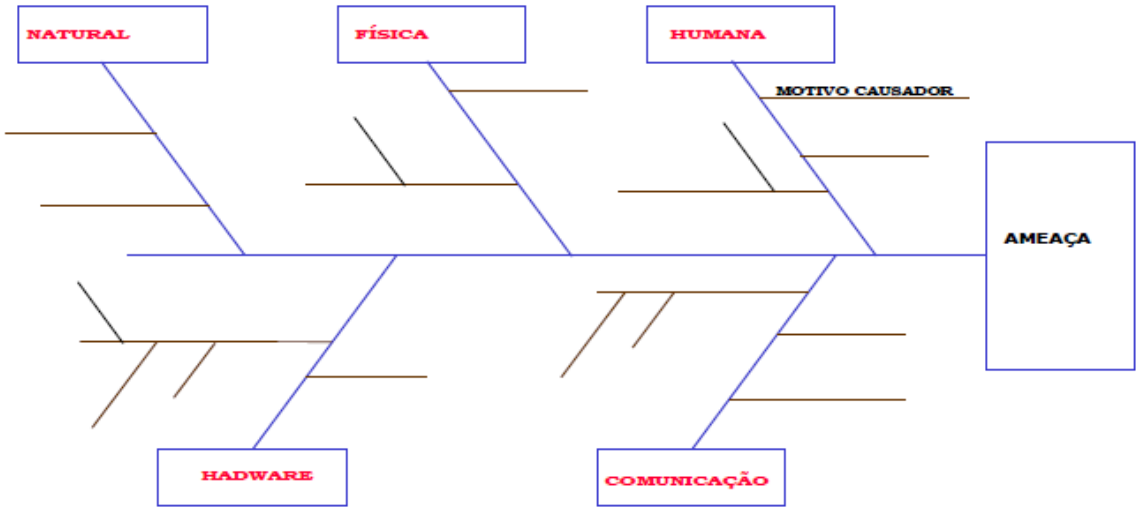

Figura 2: Diagrama de Ishikawa, adaptado (Dantas, 2011)

A auditoria é também uma outra ferramenta, que pode ser utilizada para avaliar se os controles são eficazes, e assim mensurar se estão ou não vulneráveis.

Identificar os impactos

Segundo Dantas (2011) ao se identificarem os impactos, devem ser consideradas as actividades e os critérios definidos para os requisitos de confidencialidade, integridade e disponibilidade nessas actividades.

Ainda segundo Dantas (2011) o método OCTAVE (*Operational Critical Threat, Asset, and Vulnerability Evaluation*)[1] apresenta um esquema simples, que pode facilitar a identificação de impactos.

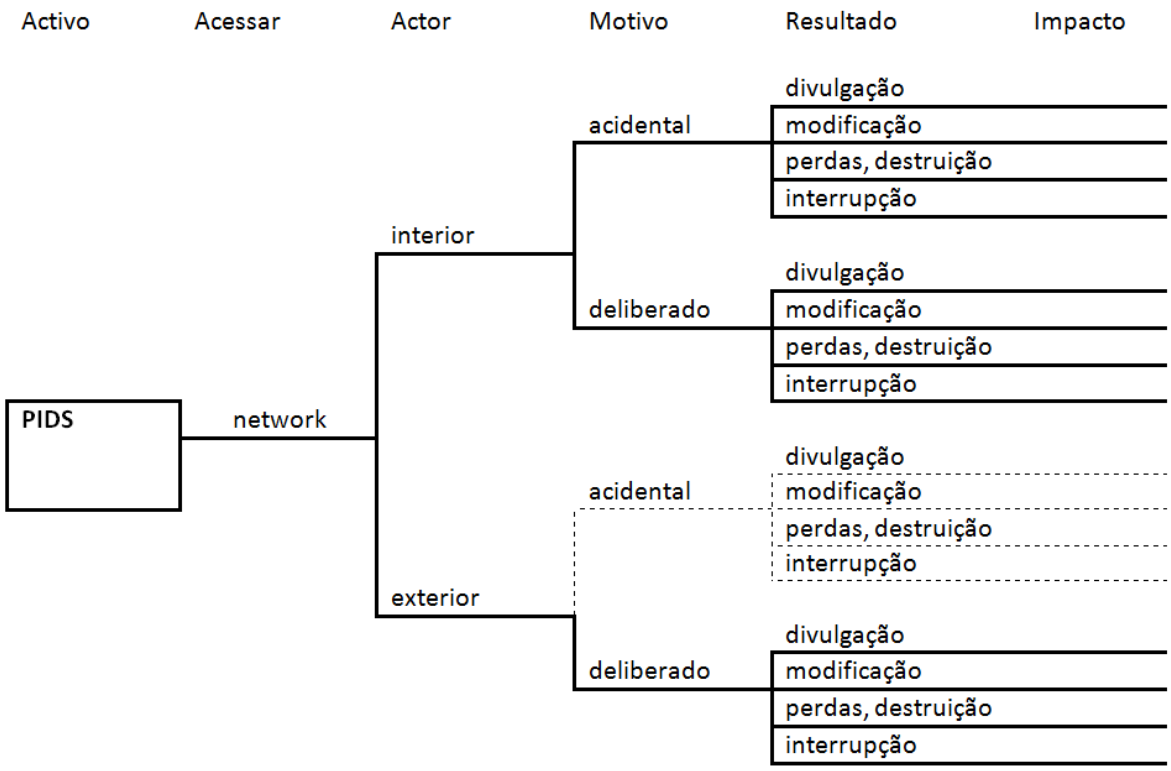

Figura 3: Método OCTAVE, adaptado (Dantas, 2011)

Analisar os riscos

A análise de riscos desenvolve um entendimento sobre os riscos e os seus impactos nas actividades de negócios e activos envolvidos, no sentido de orientar as melhores estratégias para o tratamento dentro da relação custo benefício.

Dantas (2011) entende que três factores são fundamentais: os controlos, a probabilidade e as consequências, devendo ser elaborada uma matriz de risco.

[1] "*Operational Critical Threat, Asset, and Vulnerability Evaluation* é um método de avaliação de riscos de segurança da informação que foi desenvolvido pelo *Software Engineering Institute* da *Carnegie Mellon University*. Patrocinado pelo *U.S. Department of Defense*, esse método é baseado num conjunto de critérios. Ele define os elementos fundamentais para uma avaliação de riscos de segurança de uma organização" Dantas (2011).

Valor do activo	***Níveis de ameaças***								
	Baixo (B)			**Médio (M)**			**Alto (A)**		
	Níveis de Vulnerabilidade								
	B	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Tabela 1: Matriz de riscos (V. A vs. N. A e V), adaptado (BS 7799-3:2006)

	Consequências				
Possibilidade	**Insignificante**	**Menor**	**Moderado**	**Maior**	**Catastrófico**
	1	**2**	**3**	**4**	**5**
A (Frequente)	M	A	A	E	E
B (Provável)	M	M	A	A	E
C (Ocasional)	B	M	A	A	A
D (Remota)	B	B	M	M	A
E (Improvável)	B	B	M	M	A

Tabela 2: Matriz de riscos (P vs. C), adaptado (HB 436:2004)

Níveis de ameaças	***Baixo (B)***			***Médio (M)***			***Alto (A)***		
Níveis de vulnerabilidade	B	M	A	B	M	A	B	M	A
Valor da possibilidade	0	1	2	1	2	3	2	3	4

Tabela 3: Matriz de riscos (A, V e P), adaptado (HB 436:2004)

Avaliar os riscos

É realizada uma comparação entre a classificação de cada risco analisado e o critério de avaliação estabelecido pela organização quando da escolha do método de avaliação.

Dantas (2011) define vários parâmetros utilizados na escolha dos critérios para se avaliarem os riscos, como, por exemplo:

- Financeiros;
- Imagem organizacional;
- Social e ambiental;
- Pessoal; normativo, etc.

3.5 Prevenção vs. Reacção

Segundo Dantas (2011), dois aspectos devem ser levados em consideração no estudo do risco: a prevenção e a reacção.

A prevenção engloba o conjunto de acções que objectiva evitar e detectar a possibilidade de eventos danosos aos negócios enquanto que a reacção é caracterizada pelas acções de resposta e diz respeito à adopção de medidas a partir da ocorrência de um evento segundo Dantas (2011).

3.6 Métodos de análise

A escolha do método deve ser realizada sob 2 prismas: o qualitativo e o quantitativo.

Segundo Dantas (2011) a análise qualitativa é geralmente utilizada quando não existe a disponibilidade de dados, ou quando eles são precários, e a sua análise é realizada com base em valores referenciais.

Por outro lado, a análise quantitativa é utilizada quando os dados são confiáveis e estão disponíveis, e a sua análise é realizada com base em valores absolutos relata Dantas (2011).

Landoll (2011) entende que uma das diferenças mais notáveis entre as várias técnicas de avaliação de risco de segurança é a maneira em que as variáveis de decisão são determinados ou calculados, sendo estes incluem pelo menos os seguintes aspectos:

- Valor do activo
- Probabilidade de que uma vulnerabilidade seja explorada
- Gravidade do impacto

3.6.1 Método quantitativo

Na perspectiva de Wheeler (2011), abordagens de análise quantitativa incidem sobre números concretos e cálculos para determinar a exposição ao risco. Muitas fórmulas têm sido propostas, incluindo:

- Sensibilidade × Impacto × Probabilidade = Exposição de Risco
- Taxa de Exposição = Impacto × Ameaças

Wheeler (2011) afirma que pesquisadores têm até mesmo fórmulas que inclui seis variáveis:

- Vulnerabilidade
- Popularidade
- Exposição
- Ameaças
- Valor dos activos
- Sistema

Ainda segundo Wheeler (2011) há muitos factores a considerar quando se quer medir o risco. Ele define o próximo exemplo como sendo um dos cálculos mais comum na medição dos riscos:

Expectativa de Perda Única × Taxa Anual de Ocorrência = Expectativa de Perda Anual

A fórmula calcula a expectativa de perda anual com base em uma expectativa de perda única e Taxa Anual de Ocorrência.

Por sua vez Landoll (2011) define a análise quantitativa como uma abordagem que se baseia em fórmulas e cálculos específicos para determinar o valor das variáveis de decisão de risco de segurança.

Existem várias fórmulas que são comummente associados com a análise quantitativa de riscos de segurança.

Landoll (2011) define três fórmulas clássicas para análise quantitativa de riscos de segurança, expectativa de perda anual, a expectativa de perda única, e o valor salvaguardado:

1. **Expectativa de Perda Anual** (ALE) = **Expectativa de Perda Única** × **Taxa Anual de Ocorrência**
2. **Expectativa de Perda Única = Valores do Activo × Factor de Exposição**
3. **Valor Salvaguardado = ALE Antes × ALE Depois × Custo Anual Salvaguardado**

"Expectativa de perda única (LES) é a perda esperada, como resultado de um único incidente." Landoll (2011).

Expectativa de Perda Única = Valores do Activo × Factor de Exposição

Landoll (2011) entende que alguns eventos de risco de segurança, por exemplo, vírus, acontecem várias vezes por ano, enquanto outros, como um incêndio em um armazém acontecem apenas uma vez a cada 20.

Expectativa de Perda Anual (ALE) = **Expectativa de Perda Única** × **Taxa Anual de Ocorrência**

Na perspectiva de Landoll (2011) uma medida preventiva é qualquer mecanismo de segurança administrativa, física ou técnica que reduz o risco de segurança para os activos da organização.

Valor Salvaguardado = (ALE Antes - ALE Depois) - Custo Anual de Contra medida

Landoll (2011) relata as vantagens e desvantagens da análise quantitativa.

Vantagens da análise quantitativa

- Objectivo
- Expresso em número real
- De mais fácil compreensão
- Estatísticas significativas
- Credibilidade
- Fornece uma base para a Análise Custo-Benefício
- Suporte a Decisões de Orçamento

Desvantagens da análise quantitativa

- Complexo
- Os cálculos díficel de entender
- Resultados não confiáveis
- Muito trabalho
- Falsa sensação de Precisão

3.6.2 Método qualitativo

Segundo Wheeler (2011) a maioria das abordagens qualitativas utilizam uma escala relativa (por exemplo, baixa moderada a alta) para classificar os riscos com base em alguns critérios pré-definidos para cada nível.

Por outro lado, Wheeler (2011) entende que muitos modelos quantitativos têm sido propostos mas isto depende sobre tudo dos dados históricos precisos sobre violações anteriores e, em compreender alguns conceitos avançados matemáticos.

Uma alternativa para a abordagem quantitativa é a construção de um modelo simples em torno de uma escala qualitativa e utilizar a matriz de risco, para determinar o nível de exposição final risco.

Probabilidade	Impacto		
	Alto	**Médio**	**Baixo**
Alto	Alto	Alto	Médio
Médio	Alto	Médio	Baixo
Baixo	Médio	Baixo	Baixo

Tabela 4: Tabela de mapeamento qualitativo, adaptado (Wheeler, 2011)

Landoll (2011) entende que quando um método de análise qualitativa utiliza números como valores das variáveis de risco, estes números são considerados números ordinais.

Ainda segundo Landoll (2011), os números ordinais têm ordem significativa (por exemplo, Alto> Médio> Baixo), mas não há nenhuma métrica para determinar a distância entre as categorias.

"Variáveis de equação de risco de segurança qualitativas não são expressas em termos de valores monetários, mas como uma categoria ordenada de perda monetária tais como "crítica", "Alta", "Média" e "Baixa"". Landoll (2011).

Nível de Gravidade do Impacto	***Probabilidade de ocorrência de Vulnerabilidade***				
	A Frequente	B Provavél	C Concebível	D Improvável	E Remoto
1	Risco 1	Risco 1	Risco 1	Risco 2	Risco 3
2	Risco 1	Risco 1	Risco 2	Risco 2	Risco 3
3	Risco 1	Risco 2	Risco 3	Risco 3	Risco 3
4	Risco 3	Risco 3	Risco 4	Risco 4	Risco 4

Tabela 5: Determinação do risco qualitativo, adaptado (Landoll, 2011)

Landoll (2011) relata as vantagens e desvantagens da análise qualitativa.

Vantagens da análise qualitativa

- Simples
- Valores de medição simples
- Fácil de compreender e transmitir
- Fornece adequada identificação de áreas problemáticas

Desvantagens da análise qualitativa

- Resultados subjectivos
- Valor Patrimonial Subjectiva
- Recomendações subjectivas
- Dificuldade para Traçar Melhorias

3.7 Modelos de gestão de riscos

Na perspectiva de Dantas (2011), a gestão de riscos é um processo que comporta um conjunto de actividades voltadas para o controlo dos riscos. Esse processo possui fases específicas que variam de acordo com o modelo escolhido.

3.7.1 Modelo segundo a norma ISO Guide 73:2002

Segundo a norma ISO/IEC Guide 73:2002, a gestão de riscos envolve as seguintes etapas: a avaliação de riscos (risk assessment), o tratamento do risco, a aceitação do risco e a comunicação do risco.

Avaliação de Risco - (*risk assessment*) envolve a análise de riscos (*risk analysis*) e a sua avaliação (*risk evaluation*) para se estabelecer o nível do risco.

Tratamento de Risco - (*risk treatment*) compreende as acções para modificar o risco, decisões a respeito dos riscos que afectam a organização são tomadas.

Aceitação do Risco - (*risk acceptance*) está relacionada com a capacidade da empresa de aceitar determinado risco.

Comunicação do Risco - envolve a troca de informação dos seus riscos responsáveis da alta administração, *stakeholders* e grupos de respostas a incidentes.

Gestão de Risco (3.1.7)	
	Avaliação de Risco (3.3.1)
	Análise de Risco (3.3.2)
	Identificação de Fontes (3.3.4)
	Estimativa do Risco (3.3.5)
	Avaliação de Risco (3.3.6)
	Tratamento de Risco (3.4.1)
	Evitar Riscos (3.4.6)
	Optimização de Riscos (3.4.3)
	Transferência de Risco (3.4.7)
	Retenção de Risco (3.4.9)
	Aceitação de Risco (3.4.10)
	Comunicação de Risco (3.2.4)

Figura 4: Etapas de G.R. ISO/IEC Guide 73:2002, adaptado (ISO/IEC Guide 73:2002)

3.7.2 Modelo segundo a norma AS/NZS 4360:2004

A norma AS/NZS 4360:2004 estabelece as seguintes etapas para o processo de gestão de riscos: comunicação e consulta; estabelecer o contexto; avaliar o risco (*risk assessment*); tratar o risco, monitorar e rever.

Comunicar e Consultar - estabelece a troca de informações constante e interactiva entre as partes envolvidas durante todo o processo de gestão dos riscos.

Estabelecer o contexto - abarca actividades de estabelecimento do contexto interno externo e de gestão de riscos.

Avaliação de Riscos - é identificada, analisados e avaliada os riscos de acordo com critérios previamente estabelecidos.

Tratamento de Risco - compreende acções específicas para reduzir perdas potenciais e aumentar os seus benefícios.

Monitorar e Rever - possui a característica específica de interagir em todas as fases do processo de gestão de risco.

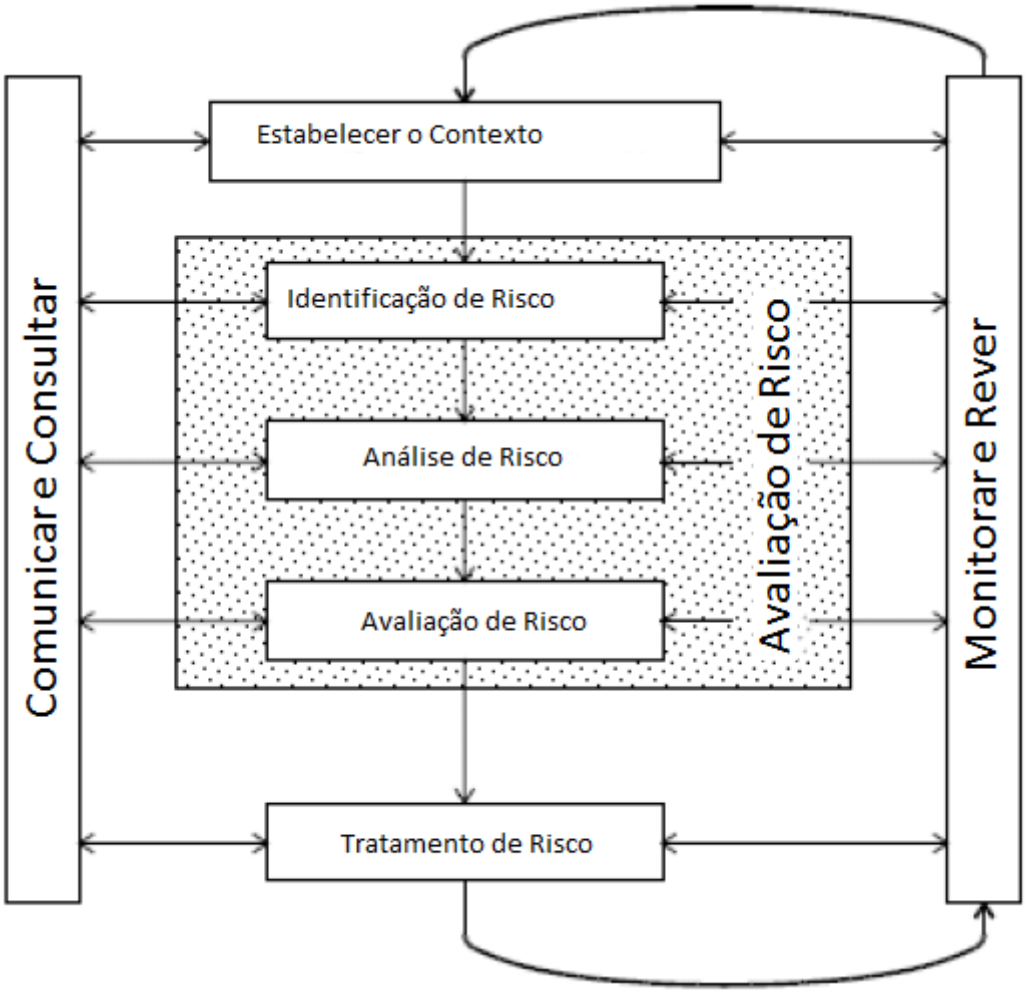

Figura 5: Etapas de G.R. AS/NZS 4360:2004, adaptado (AS/NZS 4360:2004)

3.7.3 Modelo segundo o IT Governance Institute (COBIT 4.1)

O IT Governance Institute, com a publicação do Control Objectives for Information and related Technology (COBIT® 4.1), fornece boas práticas por meio de uma estrutura de processos, domínios e actividades de controle voltadas para a boa governação nos serviços de TI.

O modelo Cobit 4.1 apresenta as seguintes etapas:

Estabelecer a estrutura de gestão de riscos - a estrutura para gerir os riscos de TI tem de estar alinhada com a estrutura de gestão de riscos da organização.

Estabelecer o contexto dos riscos - são desenvolvidas actividades para que o resultado da avaliação de riscos produza resultados apropriados.

Identificar os eventos - são identificados com as suas probabilidades e consequências.

Avaliar os riscos - ocorre a avaliação dos riscos identificados.

Responder aos riscos - ocorre o tratamento dos riscos para evitar, reduzir, compartilhar ou aceitar os riscos.

Manter e monitorar o plano de acção dos riscos - acontece a monitorização de todas as actividades de controlo, de modo a se fazerem as alterações necessárias a gestão dos riscos.

3.7.4 Modelo segundo a norma ISO 27005:2008

A ISO 27005:2008 fornece directrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um sistema de gestão de segurança da informação de acordo com o padrão da norma ISO 27001:2005.

Esse modelo apresenta as seguintes etapas:

- Definição do contexto;
- Avaliação de riscos (*risk assessment*), com as etapas de análise de riscos e avaliação de riscos (*risk evaluate*);
- Tratamento de risco;
- Aceitação do risco;
- Comunicação do risco e a Monitoração e análise crítica de riscos.

O processo de gestão de riscos é alinhado com o processo do sistema de gestão de segurança da informação de acordo com o padrão estabelecido na norma ISO 27001:2005[2], que adopta o sistema PDCA.

Processo (ISMS)	***Processo de Gestão de Segurança da Informação.***
Planear (P)	Definição do Contexto; avaliação (risk assessment); definição do plano de tratamento do risco; aceitação do risco.
Executar (D)	Implementação do plano de tratamento do risco.
Verificar (C)	Monitorização contínua e análise crítica de riscos.
Agir (A)	Manter e melhorar o processo de gestão de riscos de segurança da informação.

Tabela 6: ISMS ISO/IEC 27005:2008, adaptado (ISO/IEC 27005:2008)

3.7.5 Modelo segundo a norma BS 7799-3:2006

A norma British Standard (BS 7799-3:2006) fornece orientação e recomendações para as actividades de gestão de riscos do sistema de gestão de segurança da informação (ISMS).

Avaliação de Risco - compreende o processo de avaliação de riscos e inclui a análise e a avaliação (*evaluation*) dos riscos.

Tratamento de Riscos - decisões para gerir os riscos, por meio de controlos de prevenção e detecção, além de medidas para se evitarem e transferirem riscos.

Monitorar e rever os riscos - actividades que garantem o funcionamento eficaz dos controles implementados são estabelecidas.

Manter e melhorar os controlos de Risco - são implementados acções preventivas e correctivas.

[2] "Esta norma internacional foi preparada para fornecer um modelo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um sistema de informação de Gestão de segurança (SGSI). O adopção da (SGSI) deve ser uma decisão estratégica de uma organização. A concepção e implementação de (SGSI) de uma organização são influenciadas por suas necessidades e objectivos, requisitos de segurança, os processos empregados e o tamanho e estrutura da organização. Estes e os seus sistemas de suporte devem mudar ao longo do tempo. Espera-se que uma aplicação (ISMS) seja dimensionada de acordo com as necessidades do organismo, por exemplo, uma situação simples requer uma solução SGSI simples" ISSO/IEC 27001:2005.

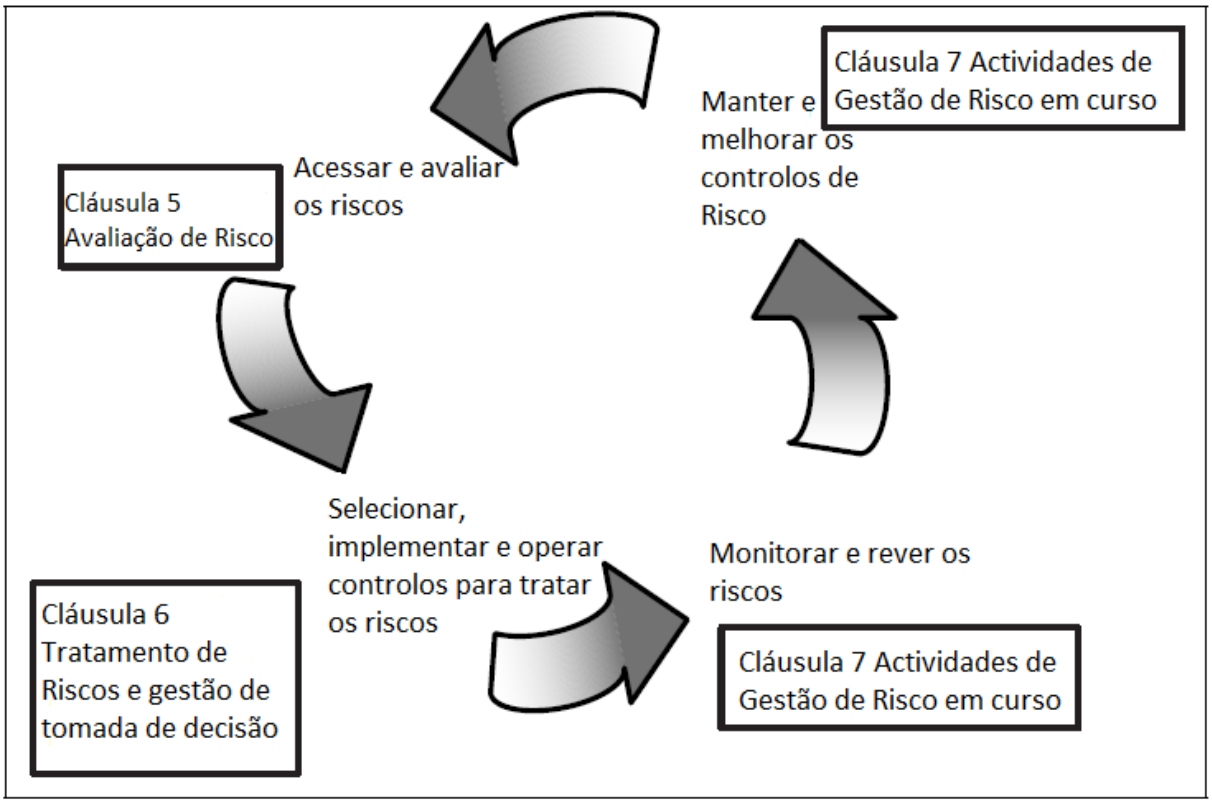
Cláusula 7 Actividades de Gestão de Risco em curso
Manter e melhorar os controlos de Risco
Acessar e avaliar os riscos
Cláusula 5 Avaliação de Risco
Selecionar, implementar e operar controlos para tratar os riscos
Monitorar e rever os riscos
Cláusula 6 Tratamento de Riscos e gestão de tomada de decisão
Cláusula 7 Actividades de Gestão de Risco em curso

Figura 6: Etapas G.R. BS 7799-3:2006, adaptado (BS 7799-3:2006)

Capítulo 4: Política de Segurança da Informação

A abordagem desse capítulo inicia pela definição do conceito de política de segurança da informação e o propósito da mesma.

Entendido o conceito da PSI, é igualmente importante retratar as características que a mesma deve possuir, baseado na visão de dois autores diferentes, Siewert (s/d) e Boavida (2000).

Como todo objecto de estudo, deve-se entender a importância da mesma, sendo verdade encontra-se diversos pontos de vista em relação a importância de uma PSI.

Conhecendo a importância de uma PSI, resta também descrever os tipos de políticas que podem ser implementados numa organização, tais como refutatória, consultiva e informativa.

Já entrando no processo de formulação de uma PSI, o capítulo retrata os níveis que uma política esta sujeita, níveis essas que englobam a alta administração passando por técnicos e demais intervenientes no processo de segurança. Cada nível está relacionado a definição de directrizes, normas e procedimentos demostrado no diagrama de conceito da política de segurança da informação.

O processo de formulação de uma PSI abarca os conceitos chaves, onde Carneiro (2002) entende a inclusão de três capítulos importantes na formulação de uma PSI, a finalidade, o conteúdo e a implementação. Mas além de Carneiro (2002) também pode-se encontrar neste capitulo as recomendações do código de boas práticas a gestão de segurança da informação a ISO/IEC 27001:2005.

Finaliza-se o capítulo com uma breve exemplificação dos modelos de segurança, modelos tais como Bell-LaPadula de David Bell e Len LaPadula, Biba de Kenneth J. passando pelo modelo Chinese Wall de Brewer and Nash.

4.1 Políticas de Segurança da Informação

Na perspectiva de Carneiro (2002) as políticas de segurança incluem documentos que descrevem a forma adequada de utilização dos recursos, as responsabilidades dos intervenientes, apresentam o que devem ser protegidos e descrevem os procedimentos a manter e desenvolver tudo com o objectivo de garantir a segurança.

"A Política de Segurança é apenas a formalização dos anseios da empresa quanto à protecção das informações" Abreu (2002) apud Laureano (2005).

> *"Em um país, temos a legislação que deve ser seguida para que tenhamos um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia. Não havia como ser diferente em uma empresa. Nesta precisamos definir padrões de conduta para garantir o sucesso do negócio Abreu (2002) apud* Spanceski (2004)"

Tal como Abreu (2002) apud Laureano (2005), podemos considerar a PSI como sendo conjunto de directrizes, normas ou leis que regem o bom funcionamento das actividades dentro da organização, lutando pela segurança dos activos da mesma.

A existência de uma boa política dentro da organização, pode repudiar as más práticas, que levam por sua vez a existência de vulnerabilidades no ceio da instituição.

> *"A política de segurança é um mecanismo preventivo de protecção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerência e pelos usuários, internos ou externos. Pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais* (Dias, 2000) apud Laureano (2005)".

Para Laureano (2005) uma política de segurança atende a vários propósitos:

- Descreve o quê e porquê esta sendo protegido;
- Define prioridades e custo do que esta sendo protegido;
- Estabelece um acordo com várias partes na empresa, no que diz respeito ao valor da segurança;
- Define regras válidas para dizer "não" quando necessário; Proporciona ao departamento de segurança a autoridade necessária para sustentar o "não";
- Impede um desempenho fútil do departamento de segurança.

Na visão de Carneiro (2002) as políticas devem garantir o cumprimento de todos os serviços de segurança:

- A Autenticação
- A Confidencialidade
- A Integridade
- A Ausência de rejeição
- A Disponibilidade dos recursos a entidades devidamente credenciados
- E o Controlo de acesso

4.2 Características de uma política

Segundo Siewert (s/d) uma política de segurança da informação não deve ser elaborada se não tiver as seguintes características:

- **Simples –** de fácil leitura e entendimento;

- **Objectiva –** deve especificar os objectos que a política retrata e estabelecer normas pontuais, devendo não ser extensas;
- **Consistente –** a política de segurança deve estar em conformidade com as leis vigentes;
- **Definição de metas –** a política de segurança deve estabelecer expectativas específicas de segurança ou seja meta;
- **Definição de responsabilidades –** deve-se definir os responsáveis pela informação e pela sua correcta utilização;
- **Definição de penalidades** – a política deve explicar a forma de punição, advertências e punições.

Por sua vez Boavida et al (2000) entende que as principais regras para a definição de uma boa política de segurança podem resumir-se no seguinte:

- Ser facilmente acessível a todos os membros da organização;
- Definir os objectivos de segurança;
- Definir objectivamente todos os aspectos abordados;
- Definir a posição da organização em cada questão;
- Justificar as opções tomadas;
- Definir as circunstâncias em que é aplicada cada uma das regras;
- Definir os papéis dos diversos agentes da organização;
- Especificar as consequências do não comprimento das regras definidas;
- Definir o nível de privacidade garantido aos utilizadores;
- Identificar os contactos para esclarecimento de questões duvidosas.

4.3 Importância de uma política de segurança

A norma ISO/IEC 27002:2005 entende que objectivo de uma PSI é fornecer orientação e apoio a gestão de segurança da informação de acordo com requisitos de negócio e as leis e regulamentos pertinentes.

Outro benefício é que todos podem conhecer as regras impostas pela empresa, sabendo como se comportar nos mais diferentes aspectos dentro da organização, sabendo inclusive o que podem ou não fazer.

Siewert (s/d) considera que qualquer funcionário, cliente, fornecedor, ou parceiro, pode conhecer a política de segurança da informação e não apenas determinado grupo de pessoas na organização.

Segundo Campos (2006) apud Siewert (s/d), a política contribui não somente para a redução de incidentes de segurança da informação, mas também para o aumento da produtividade.

De acordo com Silva (2004) apud Siewert (s/d), a política deve ir além dos aspectos de sistemas de informação e recursos computacionais, integrando as políticas institucionais relativas à segurança em geral, às metas de negócios da organização e ao plano estratégico de informática.

Ainda segundo Silva (2004) apud Siewert (s/d), o objectivo é atingido quando o relacionamento da estratégia da organização, o plano estratégico de informática e demais projectos estiverem sincronizados.

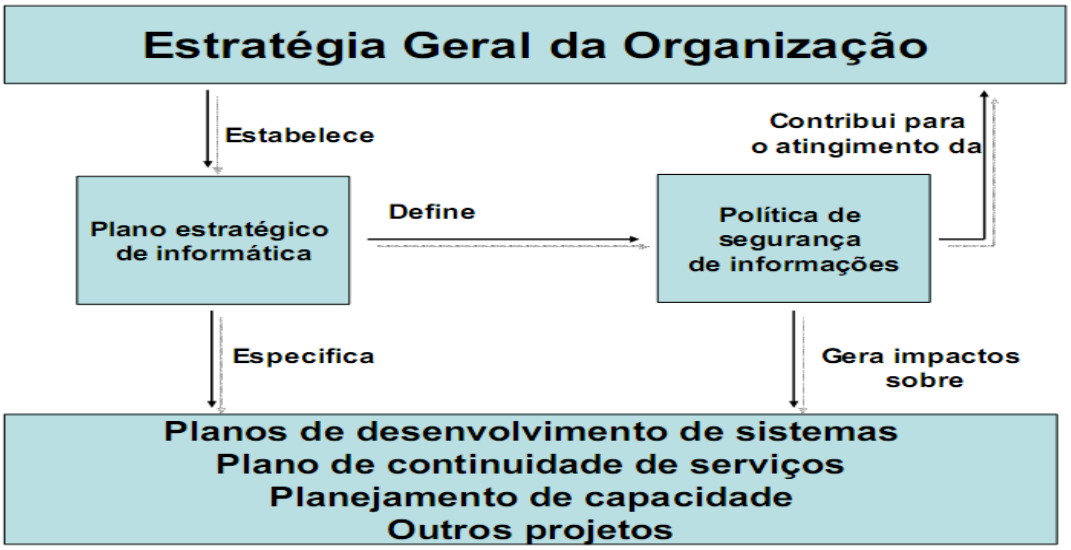

Figura 7: Relação dos objectivos de PSI, adaptado (Wadlow, 2000)

4.4 Tipos de políticas

Spanceski (2004) define a existência de três tipos de políticas diferentes, a regulatória, a consultiva, a informativa.

Refutatória

Ferreira (2003) apud Spanceski (2004) afirma que políticas refutatórias são implementadas devido às necessidades legais que são impostas à organização.

Ainda segundo Ferreira (2003) apud Spanceski (2004), as políticas refutatórias devem assegurar que a organização está seguindo os procedimentos e normas para seu ramo de actuação, provendo conforto para a organização na execução de suas actividades.

Consultiva

Spanceski (2004) afirma que as Políticas consultivas não são obrigatórias, mas recomendadas. As organizações devem conscientizar seus funcionários a considerar este tipo de política como se fosse obrigatória.

Continuando com a visão do mesmo autor, Spanceski (2004) entende que é importante que os utilizadores estejam por dentro dessas acções assim facilitando a realização de suas tarefas evitando riscos do não cumprimento das mesmas, tais como:

- Possibilidade de omissão de informações importantes para tomada de decisões críticas aos negócios da organização;
- Falhas no processo de comunicação com a alta administração;
- Perda de prazos de compromissos importantes para os negócios da organização.

Informativa

No entender de Spanceski (2004) a política informativa possui carácter apenas informativo, nenhuma acção é desejada e não existem riscos, caso não seja cumprida.

Spanceski (2004) dá um exemplo, a política pode ressaltar que o uso de um determinado sistema é restrito a pessoas autorizadas e qualquer funcionário que realizar algum tipo de violação será penalizado.

4.5 Diagrama de conceito da Política de Segurança

Segundo Dimitri (2002) apud Spanceski (2004), podemos dividir a política de segurança em três tipos: nível estratégico, nível táctico e nível operacional.

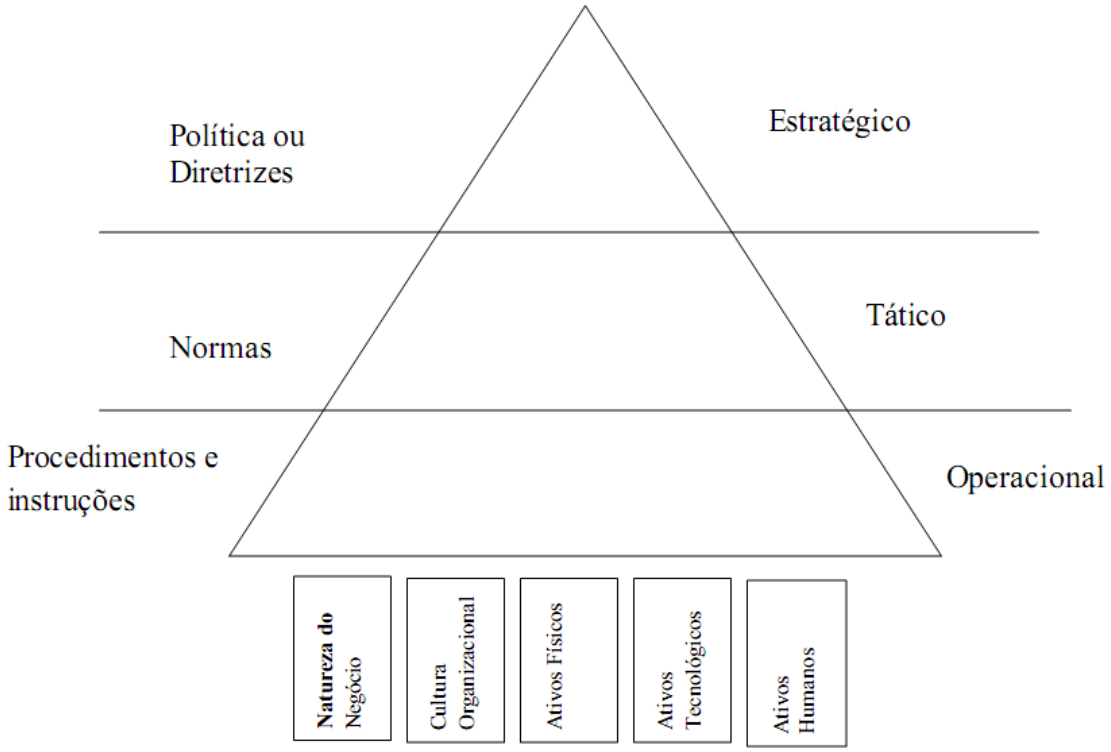

Figura 8: Diagrama de conceito dos componentes da política, adaptado (Spanceski, 2004)

Nível estratégico: refere-se ao alinhamento nos valores da empresa, ou seja, no rumo a ser seguido.

Nível táctico: para o nível táctico deve-se pensar em padronização de ambiente.

Nível operacional: deve-se garantir a perfeição no atendimento e continuidade dos negócios.

4.6 Formulação de Política de Segurança da Informação

> *"As pessoas possuem conhecimentos diferentes e aposto todas as minhas fichas que, em qualquer empresa sem uma política de segurança, a configuração de uma cidade não será igual à configuração de uma outra" Wadlow (2000) apud Laureano (2005).*

Carneiro (2002) define como necessidade a inclusão de três capítulos importantes na formulação de uma política de segurança da informação:

- Finalidades
- Conteúdo
- Implementação

4.6.1 Finalidade

A **Finalidade** segundo Carneiro (2002) deve:

- ✓ Estar integrada nas políticas globais da empresa;
- ✓ Considerar e obedecer aos objectivos;
- ✓ Apresentar o programa global da segurança em rede;
- ✓ Mostrar a importância da sua determinação de lutar contra os riscos possíveis;
- ✓ Definir as responsabilidades da implementação e manutenção;
- ✓ Apresentar as normas e padrões de comportamentos perante o SI no que se refere aos seus utilizadores.

4.6.2 Conteúdo

O **Conteúdo** ainda segundo o autor deve:

- ✓ Indicar os recursos a proteger;
- ✓ Indicar os *softwares* permitidos e a sua localização física na rede;
- ✓ Descrever os acontecimentos na presença de programas e dados que não estão homologados no sistema operativo.

- ✓ Indicar a autoria, do processo de aprovação, dos privilégios gerados e das autorizações de acesso aos diversos componentes do SI;
- ✓ Apresentação dos procedimentos necessários para garantir a informação sobre qualquer violação de segurança que possa ocorrer;
- ✓ Indicação dos gestores e a responsabilidade do ambiente operacional e dos respectivos procedimentos de controlo;
- ✓ Explicita perante os utilizadores o valor da adopção dos procedimentos de segurança, a fim de implica-los em todas as acções que garantam a segurança do SI.

4.6.3 Implementação

Carneiro (2002) entende que a **implementação** deve ser feita por conjunto de *hardware* e *software*. Programas devem possuir funções de identificação dos utilizadores, controlo de acessos e de operações além de permitir a autoria do sistema e dos procedimentos.

Ainda segundo Carneiro (2002) uma correcta implementação de uma política de segurança depende do conhecimento e cooperação dos utilizadores. Todos devem ser instruídos no sentido de saberem:

- ✓ Adoptar comportamentos adequados perante, possível violação do SI;
- ✓ A quem devem recorrer em situações que provoquem perguntas ou suspeitas;
- ✓ O que devem fazer no sentido de obterem a minimização dos riscos de segurança;
- ✓ Que políticas e medidas de segurança são estabelecidas para benefício do SI e portanto, dos seus próprios níveis de desempenho profissional.

Mamede (2006) tem a mesma visão, onde entende que o processo de segurança não é algo meramente executado por um pequeno grupo de pessoas no seio da organização, mas pelo contrário, envolve todas as pessoas da organização.

"A segurança não deve ser entediada como um conjunto de elementos tecnológicos de ponta, mas antes como algo que é aplicado de forma horizontal e consistente na organização, sendo regularmente monitorizado e avaliada" Hartley & Locke (2001) apud Mamede (2006).

Ferreira (1995) tem uma visão mais alargada do processo de desenvolvimento, onde podemos notar a diferença no acréscimo de mais processos importantes, tais como a **revisão da PSI**.

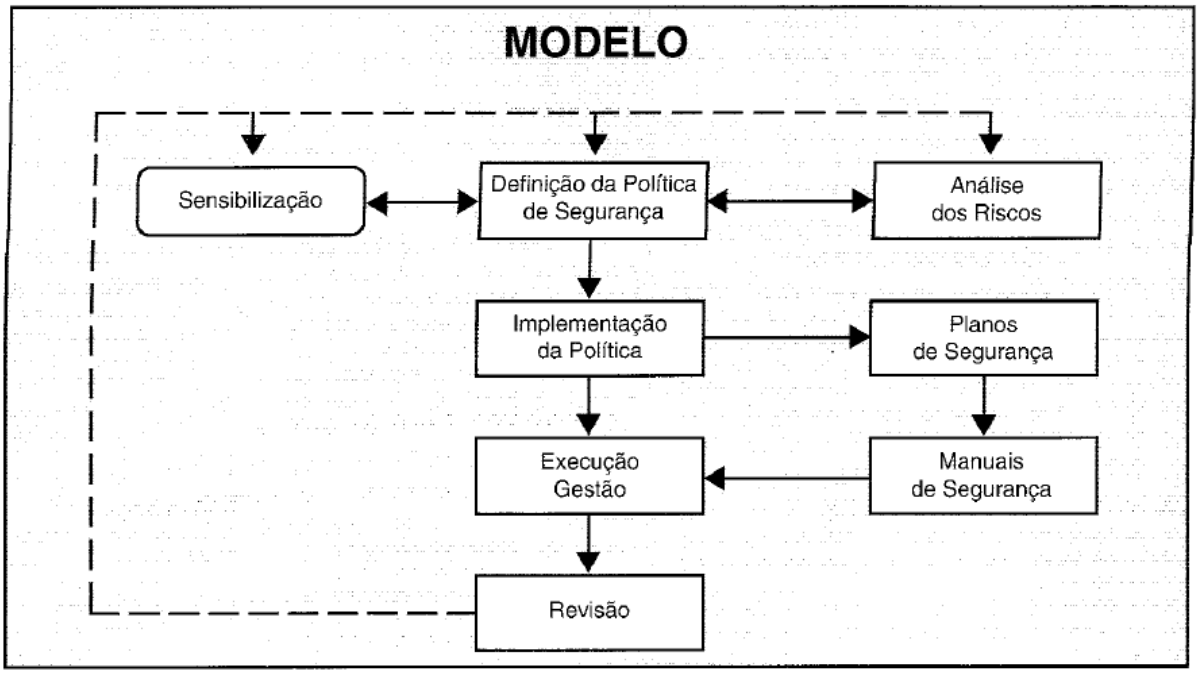

Figura 9: Modelo de Formulação de PSI, adaptado (Ferreira, 1995)

4.6.4 Revisão

A política de segurança da informação deve ser revisto a intervalos planeados ou se mudanças significativas ocorrer para assegurar a sua permanente aptidão, adequação e eficácia segundo a norma ISO/IEC 27002:2005. A política de segurança da informação deve possuir um responsável pela gestão.

A revisão deve incluir avaliação de oportunidades para melhoria da organização da PSI e abordagem de gestão de segurança da informação em resposta a mudanças no ambiente organizacional, circunstâncias de negócios, condições legais, ou ambiente técnico ainda segundo a norma ISO/IEC 27002:2005.

Continuando com as recomendações da norma ISO/IEC 27002:2005**,** a entrada para a revisão pela gestão deve incluir informações sobre:

- Realimentação das partes interessadas;

- Os resultados de avaliações independentes;
- Situação das acções preventivas e correctivas;
- Resultados de análises críticas anteriores;
- Desempenho de processo e informações sobre a conformidade política de segurança;
- Mudanças que possam afectar a abordagem da organização para a segurança;
- Tendências relacionadas a ameaças e vulnerabilidades;
- Incidentes de segurança reportados de informação;
- Recomendações fornecidas por autoridades relevantes.

A saída da revisão pela gestão deve incluir quaisquer decisões e acções relacionadas à:

- Melhoria da abordagem da organização para a segurança da informação e sua gestão processos;
- Melhoria de objectivos de controlo e controles;
- Melhoria na alocação de recursos e / ou responsabilidades.

Um registo da análise da gestão deve ser mantido. Aprovação de Gestão para a política revista deve ser obtida segundo a ISO/IEC 27002:2005.

4.7 Modelos de Segurança

Mamede (2006) entende que um modelo de segurança constitui um meio de formalização de políticas de segurança [Denning & Denning, 1998], ou seja, para a completa formulação de uma política de segurança, recorre-se a modelos onde são descritas as entidades controladas pela política e as regras que a constituem.

Ainda segundo Mamede (2006) os modelos podem ser tipificadas [Summers, 1997], segundo o seu enfoque principal, da seguinte forma:

- Confidencialidade;
- Integridade;

- Híbridos;
- Composição e não-interferência;
- Baseados em critérios de senso comum.

Como exemplos de modelos de segurança podemos referir os modelos:

- Bell-LaPadula de David Bell e Len LaPadula,
- Biba de Kenneth J.,
- Chinese Wall de Brewer and Nash.

Capítulo 5: Desenvolvimento de um modelo de PSI- o caso da Uni Piaget CV

O presente capítulo consiste no modelo de Política de Segurança da Informação desenvolvido na Universidade Jean Piaget, que pretende ser um mecanismo preventivo de protecção da informação e processos importantes na instituição em causa, pois entende-se que a PSI é o ponto de partida no processo de implementação da segurança da informação.

Também sendo este trabalho monográfico assente na temática de Gestão de Riscos, não deixamos de considerar a realização deste modelo de PSI, como sendo acções específicas para reduzir perdas potenciais e aumentar os seus benefícios (Tratamento de risco), pois um dos objectivos da etapa do tratamento de riscos no processo de avaliação de risco é assegurar a conformidade com a política de segurança da informação.

Como é sabido o processo de Gestão de risco abarca várias etapas. A necessidade da identificação dos recursos capitais da instituição levou a realização de uma avaliação/análise de risco *a priori*, sendo utilizado como base duas normas internacionais, o modelo fornecido pela norma ISO/IEC 27005:2008 e a da norma AS/NZS 4360:2004 (HB 436:2004).

Com a realização da avaliação/análise, além de ter ajudado a identificar os recursos pertinentes a serem preservados, ela também pós a nu as ameaças e vulnerabilidades que os activos estão sujeitos, podendo ainda determinar o nível de cada risco incidente na instituição.

Uma instituição universitária possui várias entidades que fazem parte do quotidiano, tais como, funcionários, docentes, alunos e colaboradores. Todas essas entidades devem participar no processo de implementação de segurança. Por ser verde, o desenvolvimento do presente modelo de PSI levou em consideração esse aspecto.

Como fonte bibliográfica utilizado na realização deste modelo de PSI tivemos:

- A norma ISO/IEC 27001:2005, ISO/IEC 27002:2005;
- Documentos e informações disponibilizados pela divisão tecnológica;
- Além de diversos modelos de Política de Segurança da Informação também consultados.

De realçar que a instituição em causa não possui nenhuma Política de Segurança da Informação implementada no ceio da organização.

5.1 Organização

A Universidade Jean Piaget de Cabo Verde é um estabelecimento de ensino superior, criado pelo Instituto Piaget, e tem como missão contribuir para a formação dos recursos humanos em Cabo Verde, bem como para o desenvolvimento de competências locais imprescindíveis para o desenvolvimento do país.

Hoje, a Universidade acolhe cerca de 2000 alunos afectos aos 16 dos 26 cursos homologados. O número de docentes ronda os 380, repartidos por vários regimes de contratação e graus académicos.

5.1.1 Órgãos de governo da Universidade

A Uni Piaget constitui-se como uma estrutura académica e administrativa. Ela está sujeita a um sistema misto de governo que reúne as responsabilidades que decorrem dos estatutos de cada instância. Os órgãos de governo são constituídos por órgãos individuais e órgãos colegiais.

5.1.2 Unidades Organizacionais

A estrutura administrativa e técnica é constituída por um conjunto de serviços que dão suporte às necessidades funcionais e operacionais da Universidade.

Serviços de Documentação – SD Exercem funções nos domínios da aquisição de obras e publicações de carácter pedagógico, científico e cultural; da recolha, tratamento e difusão de documentação e informação além da gestão da Mediateca.

Serviços Administrativos e Auxiliares – SAA Asseguram o suporte administrativo adequado ao funcionamento normal da Universidade, nas suas vertentes académica e de prestação de serviços auxiliares.

Serviços Financeiros e Sociais – SFS Encarregada da gestão financeira e patrimonial da Universidade, disponibilizam serviços de carácter social e a gestão das residências para docentes e entre outros.

Secretariado Executivo – SE Presta serviço de assessoria e secretariado à Administração, Reitoria e Órgãos Colegiais.

Gabinete de Estudos e Planeamento – GEP Auxilia a Administração e a Reitoria no planeamento e organização dos recursos técnicos e humanos e no desenvolvimento de estudos específicos.

Gabinete de Formação Permanente – GFP Espaço promotor de acções de capacitação profissional. O gabinete oferece também um serviço de formação por encomenda.

Gabinete de Comunicação e Imagem – GCI Promove a comunicação interna e externa, divulga a Universidade e suas actividades com os meios de comunicação.

Departamento de Intercâmbio e Formação Avançada – DIFA Promove a investigação científica e a formação pós-graduada.

Divisão Tecnológica – DT Assegura o funcionamento e a gestão de toda a infra-estrutura das tecnologias de informação e comunicação. Constituída por 3 secções:

- Suporte – garante a assistência técnica aos utilizadores;
- Desenvolvimento – responsável pelos *softwares* de gestão e pelo desenvolvimento de pequenas aplicações;
- Sistema – garante o funcionamento normal dos servidores e da rede multimédia da Universidade.

5.1.3 Infra-estruturas das Tecnologias de informação

Em relação a infra-estruturas das TIC´s a universidade está servida por um total de 278 computadores de mesa, 17 impressoras, 42 switch e 19 servidores, distribuídos num total de 37 unidades organizacionais.

Em termos de ligação a Internet, a universidade possui 4 linhas ADSL com uma largura de banda de 12 MB cada. Os campus da universidade dispõem de serviço de rede *wireless* a toda comunidade universitária. A universidade também está dotada de ERPs tais como a Primavera, Bibliosade e Sophia.

5.2 Avaliação de Risco

A norma ISO Guide 73:2002 entende que a Avaliação de Risco *(risk assessment*) envolve a análise de riscos (*risk analysis*) e a sua avaliação (*risk evaluation*) para estabelecer o nível do risco.

5.2.1 Análise de Risco

Segundo Ferreira (1995), o desenvolvimento de PSI deve levar em consideração a realização da análise de risco para identificar os recursos que a PSI deve preservar e conhecer os riscos aos quais a instituição esta sujeito.

5.2.1.1 Identificação de Riscos

Na realização da análise de risco foram identificados recursos (activos) pertinentes que merecem ser resguardados, pois estes contêm valores e informações relevantes da instituição. Os recursos (activos) identificados foram divididos em classes.

Recursos (activos) Físicos	***Recursos (activos) Lógicos***	***Recursos (activos) Humanos***
DT	*Software* de Gestão Primavera	Docentes
LED	Sistema de Gestão Académica	Funcionários
Laboratório de Informática	Procedimentos de solicitação de informação	Colaboradores
SD	*Software* Sofia	Alunos
SAA	Sistemas operativos	Técnicos da divisão tecnológico
SFS	Bibliosade	
SE	Procedimentos de autenticação	
GEP	Procedimentos de Cópias de Segurança	
Unidade Ciência e Tecnologia		
Sala de docentes		
Mediateca		
Reprografia		
Casa de máquinas		
PBX e extensões		
Sistemas de cablagens de rede e comunicação		
Sistema de alimentação eléctrica		
Sistema de ventilação e AC		

Bastidores Computadores Servidores Routers Switch´s UPS Dispositivos de cópias segurança Documentação e historial de alunos Documentação da rede Documentos financeiros Contabilísticos e administrativos		

Tabela 7: Recursos (Activos) Identificados

Depois de identificar os recursos (activos), foram identificados as vulnerabilidades de acordo com as classes definidas, e suas ameaças relacionadas. No processo de identificação das vulnerabilidades foram utilizados métodos tais como lista de verificação, teste ao sistema de informação, ferramentas de procura de vulnerabilidades, avaliação e testes de segurança.

As vulnerabilidades encontradas estão representadas nas tabelas que se seguem, sendo cada vulnerabilidade relacionado com as suas ameaças, os agentes de ameaças e a origem dessas ameaças. Os caracteres I,N,A nas colunas de origem, representam (N) origem natural; (I) origem intencional; (A) origem não intencional.

Vulnerabilidades de RH / Organização	***Ameaças***	***Agentes de ameaças***	***Origem***
Muitos utilizadores têm conhecimentos dos códigos de acesso ao sistema de outros utilizadores	Ex-funcionários, ex-colaboradores ou ex-alunos com credenciais de autenticação ao sistema que podem desencadear acções; Venda ou destruição de informações criticas por parte de funcionários mal-intencionados;	Pessoal interno	I
Utilizadores deixam suas secções nas suas contas abertas	Erros humanos; Espionagem por parte da concorrência;	*Hacker*; Espionagem	A, I

	Venda ou destruição de informações criticas por parte de funcionários mal-intencionados;	industrial; Pessoal interno;	
Falta de sensibilização da parte da alta direcção da Universidade sobre questões relativas à segurança da informação	Greve de pessoal informático	Pessoal interno	I, A
Funcionários mal informados e pouco sensibilizados relativamente a questões de segurança	Engenharia Social	*Hacker*; Criminoso digital; Espionagem industrial; Pessoal interno;	I, A
Pouca responsabilização por parte dos utilizadores do sistema em termos do uso do sistema de informação	Erros humanos; Degradação de materiais provocados;	*Hacker*; Criminoso digital; Pessoal interno;	I, A
Inexistência de um acordo de confidencialidade celebrado entre a organização e o funcionário	Fraude	Pessoal interno;	I
Treinamento insuficiente em segurança	Erro durante a utilização	*Hacker*; Criminoso digital; Pessoal interno;	I, A
Uso incorrecto de *software* e hardware	Erro durante a utilização	*Hacker*; Pessoal interno;	I, A
Falta de conscientização em segurança	Erro durante a utilização	Pessoal interno	I, A
Inexistência de mecanismos de monitorização	Processamento ilegal dos dados	*Hacker*; Criminoso digital; Espionagem industrial;	I
Trabalho não supervisionado de pessoal de limpeza ou de terceirizações	Furto de dispositivos e/ ou documentos	*Hacker*; Pessoal interno;	I, A
Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de equipamentos	*Hacker*; Pessoal interno;	I, A
Inexistência de um procedimento formal para o registo e a remoção	Abuso de direitos	*Hacker*	I

de utilizadores			
Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)	Abuso de direitos	*Hacker*; Pessoal interno;	I
Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros	Abuso de direitos	*Hacker*; Pessoal interno;	I
Inexistência de auditorias periódicas (supervisão)	Abuso de direitos	*Hacker*; Pessoal interno;	I
Inexistência de procedimentos para a identificação e análise/avaliação de riscos	Abuso de direitos	*Hacker*; Pessoal interno;	I, A
Inexistência de relatos de falha nos arquivos ("logs") de auditoria das actividades de administradores e operadores	Abuso de direitos	*Hacker*; Pessoal interno;	I, A
Inexistência de um processo formal para a autorização das informações disponíveis publicamente	Dados de fontes não confiáveis	*Hacker*; Pessoal interno;	I, A
Inexistência de um plano formal de continuidade	Falha de equipamentos	*Hacker*; Pessoal interno;	I, A
Inexistência de política de uso de correio-electrónico (e-mail)	Erro durante a utilização	*Hacker*; Pessoal interno;	I, A
Inexistência de procedimentos formal para a instalação de *software* em sistemas operacionais	Erro durante a utilização	*Hacker*; Pessoal interno;	I, A
Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação	Furto de equipamentos	*Hacker*; Pessoal interno;	I
Inexistência de uma política formal sobre o uso de computadores móveis	Furto de equipamentos;	*Hacker*; Pessoal interno;	I
Inexistência de controlo sobre activos fora das dependências	Furto de equipamentos	*Hacker*; Pessoal interno;	I
Política de mesas e telas limpa	Roubo de informação	*Hacker*;	I

("clear desk and clear screen") inexistente ou insuficiente		Pessoal interno;	
Inexistência de autorização para as instalações de processamento de informações	Furto de equipamentos	*Hacker*; Pessoal interno;	I
Inexistência de mecanismos completo estabelecidos para a monitorização de violações da segurança	Furto de equipamentos	*Hacker*; Pessoal interno;	I
Inexistência de análises críticas periódicas por parte da direcção	Uso não autorizado de equipamentos	*Hacker*; Pessoal interno;	I, A
Inexistência de procedimentos para o relato de fragilidades ligadas à segurança	Uso não autorizado de equipamentos	*Hacker*;	I
Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual	Uso não autorizado de equipamentos	*Hacker*; Pessoal interno;	I, A

Tabela 8: Vulnerabilidades RH/Organização e ameaças relacionadas

Vulnerabilidades Físicas	***Ameaças***	***Agentes de ameaças***	***Origem***
Pouca segurança a nível de acesso, barreiras contra acesso físico;	Assalto à Divisão Tecnológica; Acesso indevido aos recursos da rede;	*Hacker*	I
Facilidade de acesso não autorizado aos Computadores instalados nas salas de informática	Acesso indevido aos recursos da rede; Avaria de equipamentos informáticos;	*Hacker*	I
Deficiência em normas, políticas e procedimentos de segurança	Avaria de equipamentos informáticos;	Pessoal interno	I, A
Acesso descontrolado à Divisão Tecnológica	Acesso indevido aos recursos da rede; Assalto à Divisão Tecnológica;	*Hacker*	I
Não se respeita o prazo de vida dos Hardwares	Degradação do *hardware*; Incêndio provocado por curtos circuitos; Avaria de equipamentos informáticos;	Pessoal interno;	I, A
Facilidade de acesso aos	Acesso indevido aos recursos da rede;	*Hacker*	I

servidores			
Circulação de pessoas estranha na Universidade sem identificação	Assalto à departamentos;	*Hacker*	I
Pastas físicas que contêm informações críticas em locais de fácil acesso dentro da Divisão Tecnológica e LED	Acesso de pessoas não autorizadas a informações importantes;	*Hacker*	I
Facilidade de desvios de equipamentos dentro da Divisão Tecnológica	Roubos, furtos	*Hacker*; Pessoal interno;	I
Inexistência de um inventário periódico de equipamentos	Roubos , furtos	*Hacker*; Pessoal interno;	I
Portas e janelas da Divisão Tecnológica (um dos sectores mais críticos da Universidade) feita de vidro e madeira	Assalto à Divisão Tecnológica; Acesso de pessoas não autorizadas a informações importantes;	*Hacker*; Pessoal interno;	I
Cabos desarrumados e entrelaçados dentro dos bastidores e em toda a Divisão tecnológica	Degradação do *hardware;* Incêndio provocado por curtos circuitos; Avaria de equipamentos informáticos;	Pessoal interno	I, A
Falta de arrumação dos equipamentos e das ferramentas dentro da Divisão tecnológica	Roubos, furtos… Degradação do *hardware;*	*Hacker*; Pessoal interno;	
Inexistência de extintores de fogo em algumas áreas críticas ou a ausência de um documento que indica a sua localização física em toda a Universidade	Incêndio;	*Hacker*; Pessoal interno;	I, A
Falta de manutenção periódica aos equipamentos de ar – condicionado;	Incêndio provocado por curtos circuitos;	*Hacker*; Pessoal interno;	A
Inexistência de uma definição das horas que deverão ser permitidas o acesso a pessoas estranha à Divisão Tecnológica	Assalto à Divisão Tecnológica; Acesso de pessoas não autorizadas a informações importantes; Avaria de equipamentos informáticos; Avaria propositados de equipamentos informáticos;	*Hacker*; Pessoal interno;	I
Inexistência de uma Política de manutenção periódica a todos os	Degradação do *hardware;* Avaria de equipamentos informáticos;	*Hacker*; Pessoal interno;	I, A

equipamentos da Universidade			
Falta de auditoria regular e periódica à rede (física) e *hardware*	Avaria de equipamentos informáticos; Acesso indevido aos recursos da rede; Malware, *hackers*….	*Hacker*; Pessoal interno;	I
Alguns equipamentos estão expostos à incidência de raios solares durante o dia	Degradação do *hardware*; Incêndio; Avaria de equipamentos informáticos;		A
Falta de uma rotina de substituição periódica	Destruição de equipamento		A
Sensibilidade à humidade, poeira, sujeira	Poeira, corrosão, congelamento		A
Sensibilidade à radiação electromagnética	Radiação electromagnética		A
Alguns bastidores sem protecções, apenas fechados com pinos de segurança de fácil remoção e outros sem partes lateral e frontal	Acesso indevido aos recursos da rede; Avaria de equipamentos informáticos; Acesso de pessoas não autorizadas a informações importantes; Avaria propositados de equipamentos informáticos;	*Hacker*; Pessoal interno;	I, A
Inexistência de um controle eficiente de mudança de configuração	Erro durante a utilização	*Hacker*; Pessoal interno;	I, A
Sensibilidade a variações de voltagem	Interrupção de energia		
Armazenamento não protegido adequadamente	Furto de dispositivos e documentos	*Hacker*; Pessoal interno;	I
Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico	Destruição de equipamento; Vandalismo;	*Hacker*; Pessoal Interno;	I
Fornecimento de energia instável	Interrupção de energia		I

Tabela 9: Vulnerabilidades Físicas e ameaças relacionadas

Vulnerabilidades Lógicos	***Ameaças***	***Agentes de ameaças***	***Origem***
Inexistência de uma política de criação e renovação de palavras-chave	Ataques a partir da rede externa; Ataques a partir da rede interna; Acesso indevido aos recursos da rede;	*Hacker*; Espionagem industrial;	I

	Ataques e tentativas de quebras de palavra-chave;	Pessoal interno;	
Softwares e Sistemas Operativos piratas	Ataques a partir da rede interna; Ataques a partir da rede externa; Acesso indevido aos recursos da rede;	*Hacker*; Espionagem industrial;	I
Inexistência de um sistema de classificação para identificar quais as informações críticas e quais deverão ser mais protegidas e menos protegidas	Falha na Cópia de segurança; Acesso indevido aos recursos da rede; Base de Dados corrompido;	*Hacker*; Espionagem industrial; Pessoal interno;	I
Inúmeros ataques de vírus, cavalos-de-Tróia, worms nos postos	Falhas / Negação dos serviços críticos do sistema; Falha generalizada do sistema; Ataques DOS ou DDOS; Ataque de vírus, spyware e spam; Acesso indevido aos recursos da rede;	*Hacker*; Espionagem industrial;	I
Inexistência de uma política anti-fraude	Ataques a partir da rede externa; Ataques a partir da rede interna;	*Hacker*; Espionagem industrial;	I
Antenas de transmissão de rede telemóvel dentro do espaço da Universidade que podem fazer grande interferência nos sistemas informáticos	Perda acidental de dados críticos; Falhas / Negação dos serviços críticos do sistema; Falha generalizada do sistema;		
Falta de auditoria regular aos *softwares*	Ataques a partir da rede externa; Ataques a partir da rede interna;	*Hacker*; Espionagem industrial;	I
Procedimentos de teste de *software* insuficientes ou inexistentes	Abuso de direitos	*Hacker*; Espionagem industrial; Pessoal interno;	I, A
Falhas conhecidas no *software*	Abuso de direitos Alteração de *software*	*Hacker*; Espionagem industrial;	I
Não execução do "logout" ao se deixar uma estação de trabalho desassistida	Abuso de direitos	*Hacker*; Espionagem industrial;	I, A

		Pessoal interno;	
Inexistência de auditoria	Abuso de direitos	*Hacker*; Espionagem industrial; Pessoal interno;	I, A
Atribuição errada de direitos de acesso	Abuso de direitos	*Hacker*; Espionagem industrial; Pessoal interno;	I, A
Software amplamente distribuído	Comprometimento dos dados	*Hacker*;	I
Documentação inexistente	Erro durante a utilização	Pessoal interno;	I
Tabelas de palavra-passe desprotegidas	Fraudar direito de aceso	*Hacker*;	I
Serviços desnecessários permanecem habilitados	Processamento ilegal de dados; Fraudar direito de aceso;	*Hacker*; Espionagem industrial;	I
Inexistência de um controle eficaz de mudança	Defeito de *software*	*Hacker*; Espionagem industrial; Pessoal interno;	I, A
Uso não controlado de *software*	Alteração de *software*	*Hacker*; Espionagem industrial;	I, A
Inexistência de relatórios de gestão equipamentos	Utilização não autorizada de equipamentos;	Pessoal interno;	I, A
Inexistência de evidências que comprovem o envio ou o recebimento de mensagens	Repúdio de Acções	Pessoal interno;	I, A
Linhas de Comunicação desprotegidas	Sniffer na rede; Roubo de dados;	*Hacker*; Espionagem industrial;	I
Tráfego sensível desprotegido	Sniffer na rede; Roubo de dados;	*Hacker*; Espionagem industrial;	I

Tabela 10: Vulnerabilidades Lógicas e ameaças relacionadas

5.2.1.2 Estimativa do Risco

Tal como apresentado no Capitulo 3 Gestão de Riscos, independentemente do modelo escolhido para a avaliação de risco, deve-se como parte do processo, estimar os riscos, ou seja, identificar o nível de exposição do risco mediante a probabilidade de ocorrência das ameaças relacionados as vulnerabilidades sendo multiplicado pelo impacto/consequência.

Foi utilizado o método qualitativo para estimar o risco, pois entende-se que é a mais adequada fazendo face aos dados anteriormente recolhidos. Sendo método nominal, utilizou-se a escala de medição proposta pela norma Australiana/Nova Zelandesa AS/NZS 4360:2004 (HB 436:2004). As escalas de Probabilidades e a das Consequências/impacto estão abaixo apresentados.

Nível	***Descritivo***	***Definição***
5	Grave (catastrófico)	A maioria dos objectivos não pode ser atingida
4	Maior (alto)	Alguns objectivos importantes não podem ser atingidos
3	Moderado (médio)	Alguns objectivos atingidos
2	Menor (baixo)	Efeitos secundários que são facilmente corrigidas
1	Negligenciável (insignificante)	Impacto insignificante sobre os objectivos

Tabela 11: Escala de consequência, adaptado (AS/NZS 4360:2004 (HB 436:2004))

Nível	***Descritivo***	***Descrição***	***Frequência (prevista)***
A	Quase certo	O evento irá ocorrer em uma base anual	Uma vez por ano ou mais frequente
B	Provável	O evento ocorreu várias vezes ou mais em sua carreira	uma vez a cada 3 anos
C	Possível	O evento pode ocorrer uma vez em sua carreira	Uma vez em cada 10 anos
D	Improvável	O evento ocorre algures ao longo do tempo	Uma vez em cada 30 anos
E	Raro (remota)	Ouviu falar de algo parecido com o que ocorre em outros lugares	Uma vez em cada 100 anos
F	Muito raro	Nunca ouviste falar disso acontecer	Uma vez em cada 1000 anos
G	Inacreditável	Teoricamente possível, mas não se espera que ocorra	Uma vez em cada 10 000 anos

Tabela 12: Escala de probabilidade, adaptado (AS/NZS 4360:2004 (HB 436:2004))

Estando as probabilidades e consequências com escalas próprias de medição, depara-se com a necessidade de utilizar uma matriz de risco capaz de calcular o nível de cada risco. Para isso utilizou-se também como referencia, a matriz de determinação do nível de risco da norma AS/NZS 4360:2004 (HB 436:2004).

Probabilidade	***Consequências (impacto)***				
	1	**2**	**3**	**4**	**5**
A	Médio	Alto	Alto	Extremo	Extremo
B	Médio	Médio	Alto	Alto	Extremo
C	Baixo	Médio	Alto	Alto	Alto
D	Baixo	Baixo	Médio	Médio	Alto
E	Baixo	Baixo	Médio	Médio	Alto

Tabela 13: Matriz de Risco (P vs. I), adaptado (AS/NZS 4360:2004 (HB 436:2004))

A importância da matriz de risco depara na necessidade de visualizar graficamente a relação entre as probabilidades e suas consequências, e possibilitar uma identificação mais fácil dos riscos.

Já com as bases estabelecidas, resta apenas determinar o nível de risco apresentado no quadro seguinte.

Ameaças	***Probabilidade***	***Impacto***	***Nível de Risco***
Ex. Funcionários com credenciais de Autenticação de Sistemas que desencadeia acções	D	3	Médio
Ex. Alunos com credenciais de Autenticação de Sistemas que desencadeia acções	C	3	Alto
Ex. Colaboradores com credenciais de Autenticação de Sistemas que desencadeia acções	D	3	Médio
Erros humanos	B	4	Alto
Espionagem por parte da concorrência	D	3	Médio
Venda ou destruição de informações criticas por parte de funcionários mal-intencionados	C	5	Alto
Greve de pessoal informático	C	2	Médio
Engenharia Social	B	4	Alto
Degradação de materiais	C	2	Médio
Fraude	C	4	Alto
Erro durante a utilização	A	3	Alto
Processamento ilegal dos dados	C	4	Alto

Furto de dispositivos e/ ou documentos	C	4	Alto
Uso não autorizado de equipamentos	B	3	Alto
Abuso de direito	B	4	Alto
Dados de fontes não confiáveis	C	3	Alto
Falha de equipamentos	C	3	Alto
Roubo de dados ou informações	C	5	Alto
Assalto à Divisão Tecnológica	B	5	Extremo
Acesso indevido aos recursos da rede	A	3	Alto
Degradação do *hardware*	D	2	Baixo
Incêndio provocado por curtos circuitos	D	3	Médio
Assalto à departamentos	C	5	Alto
Acesso de pessoas não autorizadas a informações importantes	C	5	Alto
Avaria de equipamentos	C	3	Alto
Incêndio	D	3	Médio
Avaria propositados de equipamentos informáticos	D	3	Médio
Malware, *hackers*….	A	4	Extremo
Destruição de equipamento	D	3	Médio
Poeira, corrosão, congelamento	D	2	Baixo
Radiação electromagnética	C	4	Alto
Interrupção de energia	A	4	Extremo
Furto de dispositivos e documentos	B	5	Extremo
Vandalismo	D	2	Baixo
Ataques a partir da rede externa	A	3	Alto
Ataques a partir da rede interna	A	4	Extremo
Ataques e tentativas de quebras de palavra-chave	B	4	Alto
Falha na Cópia de segurança	C	5	Alto
Base de Dados corrompido	D	5	Alto
Falhas / Negação dos serviços críticos do sistema	C	4	Alto
Falha generalizada do sistema	C	5	Alto
Ataques DOS ou DDOS	A	3	Alto
Ataque de vírus, *spyware* e spam	A	4	Extremo
Perda acidental de dados críticos	C	5	Alto
Alteração de *software*	B	3	Alto
Comprometimento dos dados	B	4	Alto
Fraudar direito de aceso	A	3	Alto
Processamento ilegal de dados	C	3	Alto
Defeito de *software*	A	3	Alto
Utilização não autorizada de equipamentos	B	3	Alto
Repúdio de Acções	D	3	Médio
Sniffer na rede	A	4	Extremo

Tabela 14: Nível de Risco Identificados

Nota: Os valores do impacto e da probabilidade atribuídos foram baseados na opinião subjectiva, derivada da escolha do método utilizado (Método Qualitativo).

5.2.2 Avaliar o Risco

O processo de avaliar o risco (risk evaluate), incide na comparação entre a classificação de cada risco analisado e o critério de avaliação estabelecido pela organização quando da escolha do método de avaliação relata Dantas (2011).

A norma AS/NZS 4360:2004 (HB 436:2004) define como critério de avaliação o nível de atenção de administração ou a escala de tempo de resposta necessária. Por exemplo:

- **Extremo** ou **Alto risco**: necessária a atenção da alta administração, planos de acção e responsabilidade de gestão específica.
- **Risco Médio**: gerir pela monitorização específica ou procedimentos de resposta, com a responsabilidade de gestão específica.
- **Baixo risco**: gestão de rotina, dificilmente precisará aplicação específica de recursos.

5.3 Modelo de Politica de Segurança da Informação desenvolvido

Toda a organização precisa elaborar políticas restritivas e mecanismo para proteger as suas informações e garantir a segurança de toda a organização.

Sabendo disso, a formulação deste documento pretende conscientizar e preparar os intervenientes no processo de implementação da segurança da informação, sobre a importância da preservação da informação.

Ainda o referido documento inclui políticas que descreve a forma adequada de utilização dos recursos, as responsabilidades dos intervenientes, apresenta o que deve ser protegidos, os procedimentos a manter e desenvolver segundo o proposto por Carneiro (2002). Não esquecendo também que os intervenientes devem estar a par das regras impostas pela instituição, sabendo como se comportar nos mais diferentes aspectos dentro da organização, sabendo inclusive o que podem ou não fazer, tudo com o objectivo de garantir a segurança.

A segurança lógica, física e de recursos humanos deve ser levado muito a sério quando se fala da preservação da informação.

A formulação deste documento de Política de Segurança da Informação levou em conta a necessidade de preservar os recursos fulcrais da instituição, sendo dividida em três partes fundamentais, a segurança lógica, a segurança física e a segurança dos recursos humanos.

Na secção segurança lógica, podemos encontrar normas e procedimentos que auxiliam os intervenientes no processo de administração de contas, passando pela autenticação, a utilização do correio electrónico, o acesso a internet, a utilização da rede da instituição, as estacões de trabalho, a utilização de impressora, a realização de backups e a prevenção contra os vírus e malware.

Na secção segurança física elaborou-se politicas e procedimentos que devem ser seguidos no controlo de acesso, nas políticas de mesa limpa e bloqueio de ecrã à utilização dos laboratórios de informática.

Finalizando tenta-se conscientizar os intervenientes sobre a utilização da engenharia social por pessoas mal-intencionadas para conseguir informações importantes da instituição. Também tenta-se conscientizar a importância que todos os intervenientes do processo de implementação de segurança possuem na colaboração com a equipa de segurança de forma a garantir a continuidade dos negócios e que a segurança da informação seja algo que é aplicado de forma horizontal e consistente.

5.3.1 Objectivos

Garantir a segurança da informação tem sido um dos assuntos que mais preocupações têm trazido para as instituições. A confidencialidade, integridade, disponibilidade e responsabilidade da informação estão intimamente ligados à segurança.

O documento actual estabelece um conjunto de normas, instruções e procedimentos com o objectivo de normalizar e melhorar a actuação dos intervenientes na preservação dos activos institucionais ao que se refere à segurança da informação.

5.3.2 A Informação

A informação é um activo que, como qualquer outro é importante para os negócios, tem um valor para a instituição e consequentemente necessita ser adequadamente protegida.

Segundo Wheeler (2011) a informação pode ser encontrada de diversas formas, desde em formatos papéis a formatos digitais. Independentemente do seu estado (em trânsito, no processo ou em repouso) é aconselhável que ela seja protegida adequadamente.

5.3.3 Princípios da Segurança da Informação

De acordo com o modelo padrão, um sistema seguro deve garantir para a informação, três características fundamentais: a confidencialidade, a integridade e a disponibilidade.

Por outro lado diversos técnicos e estudiosos ligados a Segurança da Informação, entendem que a evolução da segurança abriu a necessidade do acréscimo de mais conceitos, a responsabilidade, a autenticidade, a ausência de rejeição entre outros.

A norma ISO/IEC 27001:2005 define essas três características de um sistema seguro:

Confidencialidade - a propriedade de que a informação não esteja disponível ou revelada a indivíduos não autorizados, entidades ou processos.

Integridade - a propriedade de salvaguardar a exactidão e plenitude dos activos.

Disponibilidade - a propriedade de ser e utilizável sob demanda por uma entidade autorizada.

5.3.4 Política de Segurança da Informação

A política de segurança inclui documentos que descrevem a forma adequada de utilização dos recursos, as responsabilidades dos intervenientes, apresentam o que devem ser protegidos e descrevem os procedimentos a manter e desenvolver, tudo com o objectivo de garantir a segurança segundo Carneiro (2002).

O Código de prática para a Gestão da Segurança da Informação ISO/IEC 27001:2005 define como objectivos de uma PSI, à de fornecer orientação e apoio a gestão de segurança da informação de acordo com os requisitos de negócios e as leis e regulamentos pertinentes.

5.3.5 Políticas de Segurança Lógica

A segurança lógica é um processo em que um sujeito activo deseja acessar um objecto passivo, envolve aspectos de prevenção contra interceptação e modificação de informações, desde sigilo no tráfego dos dados na rede, alterações de *softwares*, invasões em sistema, acessos não autorizados a informação entre outros.

Essas políticas englobam normas e procedimentos para a administração de contas, a autenticação, o correio-electrónico, o acesso a internet, a utilização de rede, estacões de trabalho, a impressora, *backup*, vírus e malware.

5.3.5.1 Administração de Contas

O processo de administração de contas abrange aspectos desde criação, manutenção à desativação de contas. Em seguida estão definidas normas e procedimentos que devem auxiliar neste processo.

5.3.5.1.1 Caracterização geral

Utilizador Administrador

Entende-se por utilizador Administrador, o responsável máximo pela gestão dos recursos da Rede.

Permissões:

- Acesso a Internet e rede interna;
- Acesso e gestão total dos recursos e serviços da rede;
- Acesso total a dados e informações dentro da rede interna;
- Acesso e administração de base de dados;

- Configuração de sistemas operacionais, aplicativos;
- Administração de computadores servidores e clientes;
- Gestão da rede interna e o acesso a Internet;
- Criação e alteração de contas e palavra-passe de utilizadores, Administradores, Suporte, Desenvolvedores, Docentes, Funcionários, Alunos e de Projecto/colaboradores.

A criação, alteração e desativação do utilizador Administrador é de inteira responsabilidade do director da divisão tecnológica. Assim como a delegação de permissões.

Utilizador Desenvolvedor

Entende-se por utilizador Desenvolvedor, os membros do Sector de Desenvolvimento de Sistemas.

Permissões:

- Acesso a rede interna e Internet;
- Acesso e administração de base de dados;
- Acesso a documentos do seu respectivo utilizador em unidade local ou remota;
- Acesso aos documentos do sector e outros sectores específicos para a realização do trabalho;
- Instalação e configuração de sistemas operacionais, aplicativos.

A criação, alteração e desativação do utilizador Desenvolvedor é de inteira responsabilidade da divisão tecnológica.

Utilizador Suporte

Entende-se por utilizador suporte, os membros do Sector de suporte de Sistemas (os funcionários técnico-administrativos e estagiários);

Permissões:

- Acesso a rede interna e Internet;
- Instalação e configuração de sistemas operacionais, aplicativos;
- Administração de computadores clientes.

A criação, alteração e desativação do utilizador Suporte é de inteira responsabilidade da divisão tecnológica.

Utilizador Docente

Entende-se por utilizador Docente, os empregados que exercem a função de professor da Universidade.

Permissões:

- Acesso a rede interna e Internet;
- Acesso aos seus documentos na unidade local ou remota;
- Acesso a documentos do sector;
- Acesso e utilização de aplicativos.

A criação, alteração e desativação do utilizador Docente é de inteira responsabilidade da divisão tecnológica. A alteração de palavra-passe será realizada pessoalmente na divisão tecnológica mediante apresentação do BI.

Utilizador Funcionário

Entende-se por utilizador Funcionário empregados da Universidade que exercem actividades técnico-administrativas.

Permissões:

- Acesso a rede interna e Internet;
- Acesso apenas a seus documentos de utilizador em unidade local ou remota;

- Acesso a documentos do sector em unidade local ou remota;
- Acesso e utilização de aplicativos e *softwares* instalados.

A criação, alteração e desativação do utilizador Funcionário é de inteira responsabilidade da divisão tecnológica. A alteração de palavra-passe será realizada pessoalmente na divisão tecnológica mediante apresentação do BI.

Utilizador Aluno

Entende-se por utilizador Aluno, todos os alunos regularmente matriculados na Universidade.

Permissões:

- Acesso a rede interna e Internet;
- Acesso apenas a seus documentos de utilizador em unidade local ou remota;
- Acesso e utilização de aplicativos e *softwares* instalados.

A criação, alteração e desativação do utilizador Aluno é de inteira responsabilidade da divisão tecnológica. A alteração de palavra-passe será realizada pessoalmente na divisão tecnológica mediante apresentação do cartão de estudante ou BI.

Utilizador de Projecto/Colaborador

Entende-se por utilizador Projecto/colaborador, todos os terceiros ou vigentes em programas/projectos e ou estagiários que necessitem de acesso aos recursos da rede.

Permissões:

- Acesso a rede interna e Internet;
- Acesso apenas a seus documentos de utilizador em unidade local ou remota;
- Acesso a documentos do sector em unidade local ou remota;
- Acesso e utilização de aplicativos e *softwares* instalados.

A criação, alteração e desativação do utilizador Projecto/colaborador é de inteira responsabilidade da divisão tecnológica. A alteração de palavra-passe será realizada pessoalmente na divisão tecnológica mediante apresentação do cartão de estudante ou BI.

5.3.5.2 Autenticação

Em praticamente todos os sistemas actuais de autenticação utilizam-se palavra-passe. Elas são utilizadas porque possuem um baixo custo.

Em contrapartida, a sua ma definição e utilização podem torna-la numa vulnerabilidade para o sistema. Muitas vezes depende do proprietário, que pode escolher palavras-passe de fácil dedução, facilitando a descoberta da mesma por pessoas mal-intencionados ou ainda compartilhar palavras-passe com amigos e conhecidos.

5.3.5.2.1 Política de palavra-passe

A *Request for Comments* (RFC) 2196, define normas para a criação de uma palavra-passe consistente.

- Não utilize palavras que estão no dicionário (nacionais ou estrangeiros);
- Não utilize informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc.;
- Não utilize palavra-passe somente com dígitos ou com letras;
- Utilize palavra-passe com, pelo menos, oito caracteres;
- Misture caracteres maiúsculos e minúsculos;
- Misture números, letras e caracteres especiais;
- Inclua, pelo menos, um carácter especial;
- Utilize um método próprio para lembrar da palavra-passe, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
- Não anote sua palavra-passe em papel ou em outros meios de registo de fácil acesso;
- Não utilize o nome do utilizador;

- Não utilize o primeiro nome, o nome do meio ou o sobrenome;
- Não utilize nomes de pessoas próximas, como da esposa(o), dos filhos, de amigos;
- Não utilize palavra-passe com repetição do mesmo dígito ou da mesma letra;
- Não forneça sua palavra-passe para ninguém, por razão alguma;
- Utilize palavra-passe que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.

As palavras-passe para os serviços disponibilizadas pela universidade devem ser sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese. Ela deve ser redefinida pelo menos a cada dois meses.

5.3.5.3 Correio-electrónico

A grande maioria das comunicações actuais tem sido feita a partir do correio-electrónico. O correio-electrónico possui processos que englobam o envio, recepção e a gestão de contas.

Devemos estar cientes que a utilização desta ferramenta acarreta contrapartidas, desde ataques informáticos, burla, assédio etc.

5.3.5.3.1 Política de correio-electrónico

O correio electrónico deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação, seja através da linguagem utilizada, frequência ou tamanho das mensagens.

Recomenda-se a contenção no envio de grande quantidade de mensagens (spam), que provoque o congestionando da rede.

Evite utilizar o correio electrónico da instituição para assuntos pessoais. Recomenda-se o envio de mensagens, no máximo para 10 destinatário de uma única vez.

Os ficheiros para anexos com mais de 10 MB devem ser compactados. Para garantir a segurança nos servidores de correio-electrónico, procedeu-se ao bloqueio das seguintes extensões*: exe, bat, src, lnk, com, dll, mpe, mpeg, mpg, pif, shs, vbs*.

Aconselha-se activar o relatório de envio das mensagens, para certificar-se que a mensagem foi recebida pelo destinatário.

Não execute ou abra ficheiros anexados com as extensões *".bat, .exe, .src, .lnk e .com"* enviados por remitentes desconhecidos ou suspeitos se não tiver solicitado.

Não devem ser enviadas mensagens de correio-electrónico cujo conteúdo seja confidencial;

Aconselha-se a manutenção da caixa de correio-electrónico, evitando acúmulo de ficheiros desnecessários.

Cada conta de utilizador tem direito à 100 MB de armazenamento no servidor de correio-electrónico.

5.3.5.4 Acesso a Internet

A Internet é uma colecção de milhares de redes interligados por um conjunto comum de protocolos de comunicações que tornam possível para os utilizadores de qualquer uma das redes comunicar, ou utilizar os serviços localizados em qualquer uma das outras redes segundo (RFC 2196).

A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos funcionários e alunos da Uni Piaget, não é permitido o seu uso para fins recreativos durante o horário de trabalho ou de aulas.

Abaixo estão definidos normas de utilização da Internet que engloba desde a navegação a *sites*, downloads e uploads de ficheiros.

5.3.5.4.1 Política de acesso a Internet

Regras Gerais

A utilização da internet deve ser racionalizado, evitando excessos que sobrecarreguem a rede e provoquem lentidão no processo de upstream e downstream de informações e prejuízo para a universidade.

Em caso de necessidade que exijam outros tipos de serviços, como *download* de ficheiros, deverão ser solicitados directamente a divisão tecnológica com autorização do administrador de rede;

Os *downloads* de ficheiros da Internet devem ser realizados através de sites confiáveis e somente os que forem necessários ao desempenho das actividades.

Serão registados em log todos os acessos a *sites*, possibilitando auditorias futuras e não é permitido burlar a estrutura de TI da instituição.

É proibido a utilização de *software* de comunicação instantânea, aplicativos que utilizam o protocolo P2P (per to per) (*uTorrent*, *kTorrent*, *bitTorrent*, etc.).

O acesso a *sites* com conteúdo pornográfico, jogos, *instant messenger*, redes sócias, é bloqueado e as tentativas de acesso serão monitorados;

Não é permitido acesso a *sites* de proxy e também a utilização de serviços de streaming (youtube etc.).

É proibido utilizar recursos da rede para deliberadamente realizar/propagar qualquer tipo de malware, *penetration test*, assédio, perturbação, ou ainda a distribuição de *softwares* cracked.

Regras para funcionários/colaboradores

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer ficheiro, *site*, correio

electrónico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A internet disponibilizada pela instituição aos seus funcionários/colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

Serão realizados relatórios dos sítios acessado, se necessário a publicação desse relatório e prestação de contas.

É proibida a divulgação e/ou o compartilhamento no domínio público na internet, de informações da área administrativa ou qualquer outra respeitante a universidade sem a autorização da alta administração.

5.3.5.5 Utilização de Rede

Garantir a segurança depende muito das protecções existentes na rede, portanto, para a utilização da rede, estão definidas normas que abrangem a autenticação, a manutenção de ficheiros no servidor e a tentativas não autorizadas de acesso. Essas normas são tanto para a rede *wireless* quanto para a rede wired.

5.3.5.5.1 Política de utilização de Redes (Wired)

Regras Gerais

Aconselha-se aos utilizadores a fazerem manutenção no directório pessoal, evitando acúmulo de ficheiros desnecessários.

Armazenamentos compartilhados, não deverão ser utilizados para guardar ficheiros que contenham assuntos sigilosos ou de natureza sensível, devem ser armazenadas apenas informações comuns a todos.

É proibido criar e/ou remover ficheiros fora da área pertencente ao utilizador e/ou que venham a comprometer o desempenho e funcionamento do sistema.

O acesso a sistemas deve ser controlado pela identificação do utilizador e pela palavra-passe, sendo as palavras-passe compartilhadas excepcionais e autorizadas pela divisão tecnológica.

Regras para funcionários

É obrigatório armazenar os ficheiros pertencentes à instituição no servidor de ficheiros para garantir a cópia de segurança dos mesmos.

Só tem a competência de efectuar a reparação dos equipamentos informáticos, os profissionais da divisão tecnológica.

A utilização de equipamentos de informática de particulares deverão ser comunicados a coordenação do departamento e a divisão tecnológica.

A quando da rescisão do funcionário, deve-se informar a divisão tecnológica, para providenciar a desativação dos acessos do utilizador à qualquer recurso da rede.

Regras para alunos

No final de cada semestre procede-se a remoção dos conteúdos nas contas de utilizador, contudo o aluno ou professor que desejar manter suas informações deve providenciar a cópia dos ficheiros sempre ao final do semestre.

Quanto a utilização de equipamentos de informática particulares o aluno deverá comunicar a coordenação de ensino responsável.

Regras para colaboradores

O acesso as informações é feito através da conta criada pela divisão tecnológica através de solicitação do coordenador responsável. Se não existir necessidade o colaborador ou estagiário pode não ter conta de acesso a rede de computadores.

O acesso a directórios ou compartilhamento dos departamentos deve ser fornecido somente em caso de necessidade de acesso.

OBS: a **Política de utilização de Redes (Wired) é complementada com as seguintes políticas retratadas neste documento:** Política de acesso a Internet e Política de utilização de estacão de Trabalho.

5.3.5.5.2 Política de utilização de Redes (Wireless)

O acesso e utilização da rede *wireless*, só poderá ser realizada dentro das instalações da universidade, mesmo que seja possível captar o sinal dessa rede fora do perímetro do campus.

O acesso a rede *wireless* só será possível mediante autenticação e apenas para alunos regularmente matriculados, docentes e funcionários/colaboradores da instituição previamente registados na divisão tecnológica.

A utilização da rede *wireless* é permitida somente para actividades académicas, de pesquisa e de extensão.

Não é permitido qualquer tipo de *scanner* na rede wireless, mesmo que seja para testes. Somente será concedido direito, mediante solicitações prévias encaminhadas para a divisão tecnológica.

É proibido qualquer tentativa de acesso não autorizado a qualquer servidor, rede ou conta da instituição ou terceiros.

É proibido desenvolver, manter, utilizar ou divulgar meios que possibilitem a violação de computadores da rede.

Não são permitidas alterações das configurações básicas de rede (IP, *Gateway*, DNS, Proxy, etc.), e a instalação de qualquer *Router*, *Access Point* ou equipamento de propagação de sinal nas instalações.

A divisão tecnológica pode acessar aos ficheiros dos utilizadores quando for indispensável para a manutenção do sistema e em falhas de segurança.

Serão responsabilizados utilizadores por qualquer dano causado à rede onde suas credenciais estiverem contidas em *logs* de acesso.

OBS: a **Política de utilização de Redes (Wireless) é complementada com as seguintes políticas retratadas neste documento:** Política de acesso a Internet e Política de utilização de estacão de Trabalho.

5.3.5.6 Estações de Trabalho

As estações de trabalho possuem códigos internos os quais permitem que ela seja identificada na rede. Qualquer acção efectuada será de responsabilidade do utilizador. Sempre que deixares de utilizar a estacão de trabalho, certifique-se que terminaste a secção.

5.3.5.6.1 Política de utilização de estacão de Trabalho

Proíbe-se nas estacões:

- Instalar jogos e aplicativos de qualquer natureza sem autorização da divisão tecnológica;
- Executar aplicativos que não sejam os instalados nos dispositivos;
- Personificar as configurações pré-definidas das estações de trabalho;
- Movimentar ou trocar os periféricos (rato, teclado, monitor etc.) ou dispositivos do lugar original;

Mantenha na sua estação somente o que for supérfluo ou pessoal. Todos os dados relativos à instituição devem ser mantidos no servidor, onde existe um sistema de *backup* diário e confiável.

5.3.5.7 Impressora

Sendo uma importante ferramenta no auxílio à realização dos trabalhos, o uso da mesma requer definição de normas, pois, as impressoras da instituição são partilhadas pelos diversos funcionários a partir da rede interna. A seguir estão definidos normas de utilização das impressoras.

5.3.5.7.1 Política de utilização de Impressora

- Devem ser utilizadas exclusivamente para impressão de documentos ou outras informações que sejam de interesse da universidade ou que estejam relacionados com o desempenho de suas actividades académicas;
- É proibida a impressão de material estritamente de interesse particular ou comercial;
- A utilização deve ser feita de forma racional e procurando não desperdiçar recursos;
- Caso a impressora emita alguma folha em branco, recoloque-a na bandeja;
- Antes de solicitar a impressão, verifique na impressora se o que foi solicitado já está impresso;
- Deve ser retirada com a maior brevidade da impressora os documentos que tenha solicitado para imprimir, que possam conter informações sensíveis da instituição;
- Não é permitido deixar impressões de qualquer informação junto às impressoras ou impressões erradas na mesa das impressoras;
- Impressões que contenham informações sensíveis que não tenham mais utilidade devem ser destruídas, visando preservar o sigilo.

5.3.5.8 Backup

O procedimento de criação de cópias de segurança é uma parte clássica de operar um sistema informático segundo (RFC 2196).

Diversos códigos de boa prática à segurança da informação recomendam a realização de *backups* regularmente nos dados e aplicativos essenciais aos negócios de forma a garantir a recuperação após um desastre ou problemas em dispositivos magnéticos. Também

recomendam-se testes regulares aos *backups* dos sistemas individuais, garantindo a satisfação dos requisitos do plano de continuidade dos negócios.

5.3.5.8.1 Política de backup

Na implementação da cópia de segurança deve-se levar em consideração a importância da informação, nível de classificação utilizado, sua periodicidade de actualização e também sua volatilidade, conforme as seguintes premissas:

- Realizar *backup* visando diminuir os riscos de continuidade;
- Manter os *backups* em local físico distante da localidade de armazenamento dos dados originais;
- Verificar a integridade da informação armazenada;
- Avaliar a funcionalidade dos procedimentos;
- Identificar procedimentos desactualizados ou ineficazes;
- Identificar falhas ou defeitos.

São de responsabilidade da divisão tecnológica os procedimentos relacionados à política de *backup*:

- Documentar, testar e avaliar regularmente as tarefas de *backup*;
- Aplicar testes de recuperação e validação dos *backups* mensalmente;
- Realizar pesquisas frequentes para identificar actualizações, novas versões do produto, ciclo de vida, sugestões de melhorias, entre outros;
- Posicionar o servidor de *backup* em local seco, climatizado, seguro e isolado, visando à segurança, integridade e inviolabilidade dos dados;
- Os dispositivos de *backup* devem ser devidamente identificadas, inclusive quando for necessário efectuar alterações nas etiquetas;
- Monitorar e controlar o tempo de vida e uso dos dispositivos de *backup*, com o objectivo de excluir dispositivos que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado ou expirando o prazo de validade;

- Formatar e testar dispositivos que apresentam erros. Caso o erro persista, deverão ser inutilizadas;
- Deverá haver um formulário de controlo rígido de execução dessas rotinas;
- Implementar procedimentos de cópias de segurança e recuperação de informações;
- Incluir no orçamento anual, a renovação dos dispositivos em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante dos dispositivos para qualquer uso de emergência.

A política de *backups*, de acordo com o serviço, deverá ocorrer da seguinte maneira:

- Diário, e de preferência incremental, nos servidores de base de dados;
- Devem ser automáticos e preferencialmente em períodos em que não haja actividade intensa na rede;
- Semanal do conteúdo dos servidores web, dns, ldap, pdc, samba, *proxy*, firewall e vpn.

5.3.5.9 Vírus e Malware

Segundo Mcclure et al (2009), Malware é geralmente aceite dentre as mais populares técnicas, como um termo que engloba todas as formas de *software* malicioso, incluindo:

- **Vírus -** programas infecciosas que podem reproduzir-se, mas exigem interacção para se propagar;
- **Worms** - programas infecciosas que podem-se auto propagar através da rede;
- **Rootkits** e **back doors -** destinados a infiltrar em sistema, esconder a sua própria presença, e fornecer controlo administrativo e funcionalidade de monitorização para um utilizador não autorizado ou atacante;
- **Bots** e **zombies** - muito semelhante ao rootkits e back doors mas focado adicionalmente em usurpar os recursos do sistema da vítima para executar uma determinada tarefa ou tarefas;
- *Software* **Cavalos de Tróia -** que faz outra coisa do que, ou em adição a, a sua funcionalidade pretendida. Normalmente, isso significa a instalação de um rootkits ou back doors.

5.3.5.9.1 Política de vírus e código malicioso

Mantenha o antivírus do seu dispositivo actualizado. Nas estacões de trabalho cabe a equipe de segurança efectuar a actualização dos antivírus, mas caso não tenha sido efectuado ou perceba que a actualização não está funcional, entre em contacto com a divisão tecnológica para que a situação possa ser corrigida.

Não é recomendado trazer dispositivos magnéticos removíveis de fora da instituição. Se não houver outra forma, certifique se não contém código malicioso.

Informe atitudes suspeitas em seu sistema a equipe técnica, para que possíveis ameaças sejam identificadas no menor espaço de tempo possível.

5.3.6 Políticas de Segurança Física

A segurança física tem como objectivo proteger equipamentos e informações contra utilizadores não autorizados a recursos institucionais, envolvendo aspectos como a prevenção contra falhas de equipamentos, incêndios, acesso de pessoas a locais restritos, enchentes, desastres naturais, acidentes, roubos e demais aspectos físicos.

Essas políticas englobam normas e procedimentos para o controlo de acesso, a mesa limpa, o bloqueio de ecrã e a utilização de laboratórios de informática.

5.3.6.1 Controlo de acesso

O controlo de acesso incide em áreas onde contêm informações e equipamentos que devem ser protegidos. As salas de servidores, os serviços financeiros e sociais, sector documental, gabinete de estudos e planeamento, sala de coordenadores e directores são áreas onde o controle de entrada é mais restrito, mas isto não significa que as demais áreas não estão contempladas.

5.3.6.1.1 Política de controlo de acesso

A divisão tecnológica só devera ser frequentada por pessoas autorizadas, sendo que os funcionários devem usar cartões de identificação.

Também nos departamentos que trabalham com informações confidenciais da instituição (sector documental, gabinete de estudos e planeamento, sala de coordenadores e directores, salas de servidores, serviços financeiros e sociais, unidades académicas), o acesso deve ser restrito a pessoas autorizadas.

A climatização das instalações que abrigam equipamentos de informática e de comunicações, devem obedecer a padrões técnicos especificado nos manuais de utilização.

Perante a perda de chaves de departamentos ou laboratórios, deve ser informada a coordenação responsável, para que possa providenciar a troca da fechadura.

5.3.6.2 Mesa limpa e Bloqueio de ecrã (clear desk and lock screen)

Os funcionários devem considerar as políticas de mesa limpa e de bloqueio de ecrã, de modo que, dispositivos removíveis, papéis e a quando da não utilização das informações nos computadores, elas sejam salvaguardados da exposição, diminuindo o risco de acesso não autorizado, perda e danos à informação.

5.3.6.2.1 Política de mesa limpa e bloqueio de ecrã

Os dispositivos magnéticos e papéis contendo informações não devem ser deixados sobre as mesas, se não estiverem a ser utilizados, devem ser guardados de maneira adequada.

A quando da não utilização das informações nos computadores, elas devem ser salvaguardados da exposição, evitando a visualização por outras pessoas que estiverem no departamento, por exemplo, pode efectuar o bloqueio de ecrã.

Material contendo informações pessoais ou institucionais, devem ser guardadas em lugares seguros.

As chaves de acesso a departamentos, laboratórios, etc., também devem ser guardadas em lugares seguros.

5.3.6.3 Utilização de laboratórios de informática

São permitidos acesso aos laboratórios somente aos alunos regularmente matriculados nos cursos de graduação e pós-graduação registados na divisão tecnológica, funcionários técnico-administrativos e aos docentes.

Os demais interessados que não constam do grupo acima referido, devem solicitar permissão perante o responsável pela coordenação dos laboratórios, disponível na secção **Membros da divisão tecnológica.**

5.3.6.3.1 Política de utilização de laboratórios de informática

A utilização dos Laboratórios de Informática tem como objectivo proporcionar suporte no processo ensino-aprendizagem desenvolvido nos cursos.

É proibida a utilização de laboratórios de informática para os seguintes efeitos:

- Instalar jogos e aplicativos de qualquer natureza;
- Executar aplicativos que não sejam os instalados nos dispositivos;
- Personificar as configurações pré-definidas das estações de trabalho;
- Movimentar ou trocar os periféricos (rato, teclado, monitor etc.) ou dispositivos do lugar original;
- Acessar a *sites* de conteúdo pornográfico;
- Acessar redes sócias;
- Utilizar telemóveis;
- Retirar material ou equipamento do Laboratório;

- Executar aplicativos que utilizam o protocolo P2P (per to per) (*uTorrent*, *kTorrent*, *bitTorrent*, etc.);
- Ouvir música com volume de som audível a outras pessoas (pode-se utilizar auscultador);
- Utilizar qualquer programa que possa comprometer a segurança da rede e dos servidores internos ou externos e o seu bom desempenho (programas *sniffer*, força bruta, *port scanner*, *malware*, DDOS etc.);
- Obter acesso não autorizado aos servidores da rede interna ou externa;
- Fazer autenticação com uma conta que não seja a do próprio utilizador
- Consumir alimentos, bebidas ou fumar cigarros.

Cada utilizador é responsável pelo equipamento no período em que estiver fazendo uso deste. O acesso deve ser controlado, somente sendo permitido o uso dos mesmos com um funcionário responsável.

Serão de inteira responsabilidade do professor orientador e dos alunos, no período no qual estiverem fazendo uso do laboratório e não houver um funcionário/estagiário responsável no local.

O funcionário responsável deve verificar se todos os computadores estão funcionando correctamente, após a utilização esta verificação deve ser repetida, qualquer problema a equipe técnica deve ser informada, para que a solução possa ser providenciada o mais rápido possível.

Os equipamentos devem ser trancados e em segurança quando deixados sem supervisão, não sendo permitida a utilização de laboratórios sem supervisão.

Se a utilização do laboratório não estiver agendada, esta utilização devera ser feita somente mediante a reserva, garantindo assim que exista um registo de utilização.

5.3.7 Âmbito Social

A engenharia social é o processo de explorar a fraqueza "humana" que é inerente a todas as organizações. O objectivo do atacante é fazer com que o empregado divulgue algumas informações que devem ser mantidas em sigilo entende Hadnagy (2011).

Os seguintes procedimentos devem ser seguidos pelos funcionários com o intuito de prevenir a engenharia social:

- Evite dialogar sobre a política de segurança da informação com pessoas de fora da instituição e em locais públicos;
- Jamais divulgue a sua palavra-passe a terceiros. A equipa técnica nunca irá solicitar a sua palavra-passe;
- Evite fazer a autenticação de serviços em dispositivos de terceiros, particularmente fora da instituição;
- Nunca execute procedimentos técnicos cujas instruções tenham sido enviados por correio-electrónico;
- Deixe a equipa técnica informada a respeito de solicitações que contradiz os tópicos anteriormente referidos.

5.3.7.1 Continuidade dos negócios

Uma informação só é valorizada se for disponibilizado em tempo útil, por isso não adianta uma informação salvaguardada se a mesma estiver inacessível. Sendo as informações activos institucionais, é necessário preserva-la independentemente do estado que se encontre (em transito, no processo ou em repouso).

O processo de segurança não é algo meramente executado por um pequeno grupo de pessoas no seio da organização, mas pelo contrário, envolve todas as entidades de dentro da instituição ou seja algo que é aplicado de forma horizontal e consistente segundo Mamede (2006).

Para garantir a continuidade dos negócios a divisão tecnológica conta com a colaboração de todos os envolvidos.

5.3.7.1.1 Membros da Divisão Tecnológica

Nome	Correio-electrónico	Telefone	Cargo
Jairson Mendes	jmendes@cv.UniPiaget.org	108	Director da DT
Carlos Tavares	ctavares@cv.unipiaget.org	110	Administrador de Sistemas
Ibraltino Moreno	imoreno@cv.unipiaget.org	111	Chefe da equipa de suporte
Ismael da Rosa	igrosa@cv.unipiaget.org	111	Técnico de suporte
Admar Correia	a04208@alunos.cv.unipiaget.org	111	Técnico de suporte estagiário

Tabela 15: Membros da Divisão Tecnológica, (DT 2013)

5.3.8 Termo de Concordância

Declaro estar ciente das determinações acima, compreendendo que qualquer não comprimento dessas normas pode implicar na aplicação das sanções disciplinares cabíveis.

Identificação do Funcionário/Colaborador/Aluno

Nome:

Nº de Identificação:

(Assinatura)

5.3.9 Verificação da utilização da política

As normas e procedimentos estabelecidos neste documento deverão ser seguidos por todos os funcionários, colaboradores e alunos, e se aplicam à informação em qualquer estado, meio ou suporte.

Para garantir as regras mencionadas acima a Uni Piaget se reserva no direito de:

- Instalar sistemas para monitorar o uso da Internet através da rede e das estações de trabalho da instituição;

- Inspeccionar dados armazenado na rede, localizados no disco local da estação ou nas áreas privadas da rede;
- As instalações estão monitoradas por câmaras de circuito interno, assegurando a identificação de qualquer delito físico efectuado dentro da instituição.

5.3.10 Violação da Política, advertência e punições

Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, a violação pode ter ocorrido por negligência, acidente ou erro; por falta de conhecimento da política ou por acção previamente determinada, ignorando a política estabelecida.

Um processo de investigação deve determinar as circunstâncias da violação, como e porque ela ocorreu.

Nos termos da Política, a Uni Piaget procederá ao bloqueio do acesso ou o cancelamento do utilizador caso seja detectado uso em não conformidade com que foi estabelecido ou de forma prejudicial à Rede, sendo a aplicação de sanções disciplinares executada de acordo com o definido nos estatutos disciplinares desta universidade, disponível em http://www.unipiaget.cv/doc/regdisciplinar.pdf.

Conclusão

O aumento crescente ao longo dos anos de ataques a segurança da informação nos mais variados sectores, leva a interrogar o caso específico da universidade. Será que ela está imune a estes possíveis ataques?

Sendo a universidade portadora de informações confidenciais tal como qualquer outra organização do mundo moderno, pensa-se ser necessário a elaboração de políticas restritivas que assegure a conformidade com a gestão de risco.

Neste contexto uma das principais motivações para a realização deste trabalho foi o de investigar detalhadamente o quão vulnerável à ameaças estará a segurança da informação da universidade.

Com a realização de uma avaliação de risco utilizando as normas ISO/IEC 27005:2008 e a AS/NZS 4360:2004 (HB 436:2004) como referência, pretendeu-se classificar os riscos presentes na instituição, servindo como base para o desenvolvimento de um modelo de PSI que esteja em conformidade com a gestão de riscos.

A escolha da norma AS/NZS 4360:2004 (HB 436:2004) não foi por acaso, pois a mesma é considerado a norma mais completa nos dias que correm, tal acontece também com a norma

utilizada para a realização do modelo de PSI a norma ISO/IEC 27001:2005, ISO/IEC 27002:2005.

Sendo assim ignorar os riscos não os faz deixar de existir. A informação é um activo da organização cuja segurança deve fazer parte de sua gestão.

Pode-se dizer que cada vez mais as organizações estão dependentes da informação, muitas vezes esquecem que também os equipamentos podem estar sujeitos a falhas, devendo esses equipamentos serem levados em consideração no plano de continuidade dos negócios. Aspectos cruciais, tais como, o valor da informação, a competitividade da empresa, o alinhamento estratégico dirão na íntegra a justificativa ou não do investimento em SI.

Tal como Dantas (2011), a gestão de riscos é um processo que comporta um conjunto de actividades voltadas para o controle dos riscos.

Sendo assim a gestão de riscos assenta em fazer com que os riscos não venham a superar aqueles que a Alta administração esteja sujeita a suportar. Esses riscos dependem do contexto, envolvendo uma vasta gama de entidades, processos e tecnologia.

Dantas (2011) entende que em um cenário de incertezas, as ameaças e oportunidades têm o potencial de produzir perdas ou aumentar os ganhos, onde os resultados positivos são obtidos com uma boa gestão de incertezas e de seus riscos, optimizando as suas oportunidades e estabelecimento de estratégias para o crescimento na busca da maximização dos resultados. Entende ainda que os resultados negativos são oriundos da falta ou da fragilidade dessa gestão, onde os resultados podem trazer perdas de grandes proporções.

Pois desta forma, o estudo de risco assume o protagonismo nas organizações actuais proporcionando-lhes um processo de gestão baseado nos ricos, onde o desenvolvimento de um documento de Política de Segurança da Informação deve estar em conformidade com o processo de tratamento do risco.

Tal como referenciado no estudo das artes deste trabalho, a PSI segundo Carneiro (2002) incluem documentos que descrevem a forma adequada de utilização dos recursos, as

responsabilidades dos intervenientes, apresentam o que devem ser protegidos e descrevem os procedimentos a manter e desenvolver tudo com o objectivo de garantir a segurança.

A PSI além de incluir esses propósitos, ela também deve ser capaz de fornecer orientação e apoio a gestão de segurança da informação de acordo com requisitos de negócio e as leis e regulamentos pertinentes entende a norma ISO/IEC 27002:2005. Também ela deve ser capaz de fornecer a todos o conhecimento das regras impostas pela empresa, sabendo como se comportar nos mais diferentes aspectos dentro da organização, sabendo inclusive o que podem ou não fazer.

Mamede (2006) tem a mesma visão, onde entende que o processo de segurança não é algo meramente executado por um pequeno grupo de pessoas no seio da organização, mas pelo contrário, envolve todas as pessoas da organização.

No final deste estudo conclui-se que em primeiro lugar o desenvolvimento de uma Política de Segurança deve estar em conformidade com a gestão de risco.

Respondendo as perguntas de partida elaboradas no início deste trabalho monográfico, pode-se concluir que, a instituição não esta dotada de um documento de Política de Segurança da Informação, sendo este o ponto de partida na implementação da segurança da informação, é recomendado que a instituição adopte um documento formal onde descreve a forma adequada de utilização dos recursos, as responsabilidades dos intervenientes, apresentam o que devem ser protegidos e descrevem os procedimentos a manter e desenvolver tudo com o objectivo de garantir a segurança segundo Carneiro (2002).

Não basta apenas a elaboração do documento, também é recomendado a correcta implementação onde Carneiro (2002) entende que implementação deve ser feita por conjunto de *hardware* e software. Ainda segundo Carneiro (2002) uma correcta implementação depende do conhecimento e cooperação dos utilizadores.

A norma ISO/IEC 27002:2005 entende que o apoio da alta administração no processo de implementação é fundamental. Ao mesmo tempo conclui-se que a universidade não possui um documento de PSI, logo a gestão de risco não esta delineado em conformidade com a PSI.

Desta forma, o caso prático realizado na Universidade Jean Piaget, mostra-nos o quanto ainda deve ser investido na segurança da informação pela alta administração da universidade.

A gestão de risco, onde foi dado maior enfâse nos processos de avaliação e análise de risco, mostra as vulnerabilidades que os activos institucionais estão sujeitos, vulnerabilidades essas que podem desencadear ameaças com um nível muito alto de risco.

A estimativa dos riscos mostrou-nos o nível de cada risco, de referir alguns, onde é necessária a atenção da alta administração, planos de acção e responsabilidade de gestão específica, pois são riscos de nível extremo ou alto. Também foram identificados riscos de nível médio que devem ser geridos pela monitorização específica ou procedimentos de resposta, com a responsabilidade de gestão específica. Por último foram identificados riscos de níveis baixo, onde precisarão de procedimentos de rotina, e dificilmente de aplicação específica de recursos.

Como referido anteriormente, concluiu-se que a instituição não possui nenhum documento formal de PSI adoptado. Espera-se que o modelo de PSI desenvolvido possa servir como base para uma futura implementação de PSI na instituição. Sendo assim o modelo levou em consideração pontos específicos de uma instituição universitária, entidades que fazem parte do quotidiano, tais como, funcionários, docentes, alunos e colaboradores. Todas essas entidades devem participar no processo de implementação de segurança.

Também o documento sugeriu a criação de políticas específicas, divididos em políticas lógicas, políticas físicas e politicas no âmbito social. Estas políticas devem ser disponibilizadas a todos os funcionários, além de serem divulgados para os alunos e demais envolvidos.

Recomenda-se também se necessário treinamentos a funcionários e demais entidades conscientizando o envolvimento de cada um na utilização adequada e na divulgação da política de segurança.

A norma ISO/IEC 27002:2005 recomenda que a política de segurança da informação deve ser revisto a intervalos planeados ou se mudanças significativas ocorrer para assegurar a sua

permanente aptidão, adequação e eficácia. Também a norma recomenda ser mantido um registo da gestão.

Finalizando, a norma ISO/IEC recomenda que a PSI deve ser devidamente formalizada perante a administração, através de um documento formal que expresse as preocupações da organização e estabeleça as linhas mestras para a gestão da segurança da informação, aprovado pela Direcção, publicado e comunicado de forma adequada a todos os intervenientes no processo de segurança da informação.

Bibliografia

Carneiro, Alberto, (2002), *Introdução à Segurança dos Sistemas de Informação, Segurança um factor de sucesso - Auditoria, Politicas e Benefícios da Segurança, Lisboa*, FCA - Editora de informática.

Dantas, Marcus Leal, (2011). *Segurança da Informação: uma abordagem focada em gestão de riscos,* Livro Rápido Olinda – PE.

Ed Skoudis and Tom Liston, (2005). *Counter Hack reloaded*, Prentice Hall, NJ.

Ferreira Jorge, colaboração de Alves Sebastião, (1995). *Manual Técnico de Segurança dos Sistemas e Tecnologias de Informação,* Instituto de Informática.

Freitas, Eduardo Mello, (2009). *Gestão de riscos Aplicada a sistemas de informação: Segurança estratégica da informação,* Universidade Candido Mendes, Brasil.

Hadnagy, Christopher, (2011). *Social Engineering: The Art of Human Hacking,* Wiley Publishing, Inc., Indianapolis, Indiana.

Landoll, Douglas J., (2011). *The Security Risk Assessment Handbook: a complete guide for performing Risk Assessment*, CRC Press.

Mamede, S. Henrique, (2006), *Segurança Informática nas Organizações,* FCA-Editora Informática, Lda.

Mcclure Stuart, Scambray Joel, Kurtz George, (2009).*Hacking Exposed 6: Network Security Secrets & Solutions*, McGraw-Hill, Companies.

Monteiro, Edmundo, Boavida, Fernando, (2000), *Engenharia de Redes Informáticas*, 4ª Edição, FCA Editora de Informática Lda.

Siewert, Vanderson C, (s/d)**.** *Integração da política de segurança da informação com o Firewall,* pós-graduação "lato sensu", publicada, Faculdade de Tecnologia do SENAI de Florianópolis.

Spanceski, Francini Reitz, (2004). *Política de Segurança da Informação - Desenvolvimento de um modelo voltado para Instituições de ensino,* monografia de Bacharelato, publicada, Instituto Superior Tupy.

Tipton, Harold F, Krause Micki, (2008). *Information Security Management Handbook,* CRC Press. Taylor & Francis Group, LLC

Wheeler, Evan, (2011). *Security Risk Management Building an Information Security Risk Management Program from the Ground Up,* Elsevier, Inc.

Young, Carl S., (2010). *Metrics and Methods for Security Risk Management,* Elsevier, Inc.

Disponíveis em linha

AS/NZS 4360:2004, disponível em <www.mwds.com/.../AS-NZS%204360-2004%20... >, [consultado em 2/01/2013].

Boas práticas em Segurança da Informação 2ª edição.pdf, disponível em <*portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF*>, [consultado em 18/09/2012].

BS 7799-3:2006, disponível em <www.iso.staratel.com/.../BS%207799-3-2006.pdf >, [consultado em 03/09/2012].

Campos, A. (s/d), *Auditoria em tecnologia da informação,* disponível em <www.4shared.com>, [consultado em 30/09/2012].

Da Rosa, Isaías. (s/d), *Segurança de Sistemas de Informação na Cidade da Praia*, disponível em <http://bdigital.cv.unipiaget.org:8080/jspui/handle/10964/241>, [consultado em 30/09/2012].

HB 436:2004, disponível em <bch.cbd.int/database/attachment/?id=12285>, [consultado em 03/09/2012].

ISO/IEC 27001:2005, disponível em <webstore.iec.ch/.../info_isoiec27001%7Bed1.0%...>, [consultado em 03/09/2012].

ISO/IEC 27002:2005, disponível em <*torrent*>, [consultado em 03/09/2012].

ISO/IEC 27005:2008, disponível em <http://pdf4share.net/isoiec-270022005-information technology-security-techniques-code-of-practice-for-information-security-management redesignation-of-isoiec-177992005/>, [consultado em 03/09/2012].

ISO/IEC Guide 73:2002, disponível em <http://www.4shared.com/get/VFiN5Jf5/ISO-IEC_Guide_73_2002_Risk_Man.html >, [consultado em 05/09/2012].

IT Governance Instituten Cobit 4.1, disponível em <http://praktische-informatik.fh-luebeck.de/sites/default/files/CobiT_4.1.pdf>, [consultado em 10/09/2012].

Laureano, P. A. M, (2005), *Gestão de Segurança da Informação,* [em linha] disponível em <*www*.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> [consultado 28/05/ 2012].

NBR ISO/IEC 27001, disponível em <http://www.vazzi.com.br/moodle/pluginfile.php/135/mod_resource/content/1/ISO-IEC-27001.pdf>, [consultado em 06/09/2012].

NBR ISO/IEC 27002, disponível em <http://freepdfdb.com/pdf/nbr-iso-27002>, [consultado em 03/09/2012].

NBR ISO/IEC 27005, disponível em <http://www.brunomoraes.com.br/governanca-em-ti/wp-content/uploads/2010/11/NBR_ISO27005_ConsultaABNT1.pdf>, [consultado em 04/09/2012].

Políticas, Modelos e Mecanismos de Segurança (s/d), disponível em <www.catalao.ufg.br> [consultado em 05/09/2012].

Políticas de Segurança (s/d), disponível em <penta.ufrgs.br>, [consultado em 03/09/2012].

Política de Segurança da Informação – Directrizes Gerais (s/d), disponível em <www2.ati.pe.gov.br>, [consultado em 03/09/2012]

Política de Segurança da Informação Unicamp.pdf, disponível em <*www.gastrocentro.unicamp.br/download/politica.pdf*>, [consultado em 15/01/2013].

Política de segurança e utilização dos recursos de rede e computacionais dos laboratórios LCI e LEA.pdf, disponível em <*www.inf.furb.br/info/Politica_Seguranca.pdf*>, [consultado em 25/01/2013].

Política de Segurança da Informação Uri.pdf, disponível em <*www.fw.uri.br/.../Política%20de%20Segurança%20da%20Informaçã...*>, [consultado em 22/01/2013].

Política de Segurança da Informação Instituto Mato Grosso do Sul.pdf, disponível em <*www.ifms.edu.br/wp.../05/política-de-segurança-da-informação.pdf*>, [consultado em 16/01/2013].

Política de Segurança da Informação Senac.pdf, disponível em <*www.sp.senac.br/.../psi_normas_administrativas.pdf*>, [consultado em 15/01/2013].

Regulamento Disciplinar Uni Piaget, disponível em <http://www.unipiaget.cv/doc/regdisciplinar.pdf>, [consultado em 28/01/2013].

Request for Comments (RFC 2196), disponível em <www.ietf.org/rfc/rfc2196.txt>, [consultado em 22/01/2013].

Anexo

I. Lista de verificação

A elaboração da lista de verificação foi baseada no anexo D da norma de boas prática à segurança da informação NBR ISO/IEC 27005. Para o seu preenchimento, utilizou-se métodos de procura de vulnerabilidade tais como, teste ao sistema de informação, ferramentas de procura de vulnerabilidades, avaliação, testes de segurança entre outros.

Vulnerabilidades físicas

- ☐ Manutenção insuficiente/Instalação defeituosa de dispositivos de armazenamento
- ☒ Falta de uma rotina de substituição periódica
- ☒ Sensibilidade à humidade, poeira, sujeira
- ☒ Sensibilidade à radiação electromagnética
- ☐ Inexistência de um inventário periódico de equipamentos;
- ☒ Alguns bastidores sem protecções, apenas fechados com pinos de segurança de fácil remoção e outros sem partes lateral e frontal;
- ☒ Pouca segurança a nível de acesso, barreiras contra acesso físico;
- ☒ Facilidade de acesso não autorizado aos Computadores instalados nas salas de informática;
- ☒ Deficiência em normas, políticas e procedimentos de segurança;
- ☒ Acesso descontrolado à Divisão Tecnológica
- ☒ Não se respeita o prazo de vida dos Hardwares;
- ☒ Inexistência de um controle eficiente de mudança de configuração
- ☒ Sensibilidade a variações de voltagem
- ☒ Sensibilidade a variações de temperatura
- ☒ Armazenamento não protegido adequadamente
- ☐ Falta de cuidado durante o descarte
- ☐ Realização de cópias não controlada
- ☒ Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico

☐ Localização em área susceptível a inundações

☒ Fornecimento de energia instável

☐ Inexistência de mecanismos de protecção física no prédio, portas e janelas

☒ Facilidade de acesso aos servidores;

☒ Circulação de pessoas estranha na Universidade sem identificação;

☒ Pastas físicas que contêm informações críticas em locais de fácil acesso dentro da Divisão Tecnológica e LED.

☒ Facilidade de desvios de equipamentos dentro da Divisão Tecnológica;

☒ Portas e janelas da Divisão Tecnológica (um dos sectores mais críticos da Universidade) feita de vidro e madeira;

☒ Cabos desarrumados e entrelaçados dentro dos bastidores e em toda a Divisão tecnológica

☒ Falta de arrumação dos equipamentos e das ferramentas dentro da Divisão tecnológica;

☒ Inexistência de extintores de fogo em algumas áreas críticas ou a ausência de um documento que indica a sua localização física em toda a Universidade;

☒ Falta de manutenção periódica aos equipamentos de ar – condicionado;

☒ Inexistência de uma definição das horas que deverão ser permitidas o acesso a pessoas estranha à Divisão Tecnológica;

☒ Inexistência de uma Política de manutenção periódica a todos os equipamentos da Universidade;

☒ Falta de auditoria regular e periódica à rede (física) e hardware;

☒ Alguns equipamentos estão expostos à incidência de raios solares durante o dia;

Vulnerabilidades lógicas

☒ Procedimentos de teste de *software* insuficientes ou inexistentes

☒ Falhas conhecidas no *software*

☒ Não execução do "logout" ao se deixar uma estação de trabalho desassistida

☐ Descarte ou reutilização de dispositivos de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados

☒ Inexistência de auditoria

☒ Atribuição errada de direitos de acesso

☒ *Software* amplamente distribuído

☐ Utilizar programas aplicativos com um conjunto errado de dados (referentes a um outro período)

☐ Interface de utilizador complicada

☒ Documentação inexistente

☐ Configuração de parâmetros incorrecta

☐ Datas incorrectas

☐ Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores

☒ Tabelas de palavra-passe desprotegidas

☒ Gestão de palavra-passe mal feito

☒ Serviços desnecessários permanecem habilitados

☐ Software novo ou imaturo

☐ Especificações confusas ou incompletas para os desenvolvedores

☒ Inexistência de um controle eficaz de mudança

☒ Inexistência de uma política anti-fraude;

☒ Antenas de transmissão de rede telemóvel dentro do espaço da Universidade que podem fazer grande interferência nos sistemas informáticos;

☒ Uso não controlado de software

☐ Inexistência de cópias de segurança

☐ Inexistência de mecanismos de protecção física no prédio, portas e janelas

☒ Inexistência de relatórios de gestão equipamentos

☒ Inexistência de evidências que comprovem o envio ou o recebimento de mensagens

☒ Linhas de Comunicação desprotegidas

☒ Tráfego sensível desprotegido

☐ Junções de cabeamento mal feitas

☐ Ponto único de falha

☐ Não identificação e não autenticação do emissor e do receptor

☐ Arquitectura insegura da rede

☐ Transferência de palavra-passe em claro

☐ Gestão de rede inadequado (quanto à flexibilidade de roteamento)

☐ Saturação do sistema de informação

☐ Conexões de redes públicas desprotegidas

☒ Inexistência de uma política de criação e renovação de palavras-chave;

☒ *Softwares* e Sistemas Operativos piratas;

☒ Inexistência de um sistema de classificação para identificar quais as informações críticas e quais deverão ser mais protegidas e menos protegidas;

☒ Inúmeros ataques de vírus, cavalos-de-Tróia, *worms;*

☒ Falta de auditoria regular aos *softwares;*

Vulnerabilidades de RH e Organização

☒ Inexistência de um acordo de confidencialidade celebrado entre a organização e o funcionário;

☐ Ausência de recursos humanos

☐ Procedimentos de recrutamento inadequados

☒ Treinamento insuficiente em segurança

☒ Uso incorrecto de *software* e hardware

☒ Falta de conscientização em segurança

☒ Inexistência de mecanismos de monitorização

☒ Trabalho não supervisionado de pessoal de limpeza ou de terceirizações

☒ Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens

☒ Muitos utilizadores têm conhecimentos dos códigos de acesso ao sistema de outros utilizadores;

☒ Utilizadores deixam suas secções nas suas contas abertas;

☒ Falta de sensibilização da parte da alta direcção da Universidade sobre questões relativas à segurança da informação;

☒ Funcionários mal informados e pouco sensibilizados relativamente a questões de segurança;

☒ Pouca responsabilização por parte dos utilizadores do sistema em termos do uso do sistema de informação;

☒ Inexistência de um procedimento formal para o registo e a remoção de utilizadores

☒ Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)

☒ Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros

☐ Inexistência de procedimento de monitorização das instalações de processamento de informações

☒ Inexistência de auditorias periódicas (supervisão)

☒ Inexistência de procedimentos para a identificação e análise/avaliação de riscos

☒ Inexistência de relatos de falha nos arquivos ("logs") de auditoria das actividades de administradores e operadores

☐ Resposta inadequada do serviço de manutenção

☐ Acordo de nível de serviço (SLA - da sigla do termo em inglês) inexistente ou insuficiente

☐ Inexistência de procedimento de controlo de mudanças

☐ Inexistência de um procedimento formal para o controle da documentação do SGSI

☐ Inexistência de um procedimento formal para a supervisão dos registos do SGSI

☒ Inexistência de um processo formal para a autorização das informações disponíveis publicamente

☐ Atribuição inadequada das responsabilidades pela segurança da informação

☒ Inexistência de um plano formal de continuidade

☒ Inexistência de política de uso de correio-electrónico (e-mail)

☒ Inexistência de procedimentos formal para a instalação de *software* em sistemas operacionais

☐ Ausência de registos nos arquivos de auditoria ("logs") de administradores e operadores

☐ Inexistência de procedimentos para a manipulação de informações classificadas

☐ Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções

☒ Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação

☒ Inexistência de uma política formal sobre o uso de computadores móveis

☒ Inexistência de controlo sobre activos fora das dependências

☒ Política de mesas e telas limpa ("clear desk and clear screen") inexistente ou insuficiente

☒ Inexistência de autorização para as instalações de processamento de informações

☒ Inexistência de mecanismos completo estabelecidos para o monitorização de violações da segurança

☒ Inexistência de análises críticas periódicas por parte da direcção

☒ Inexistência de procedimentos para o relato de fragilidades ligadas à segurança

☒ Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual

II. Guião de entrevista

1. Qual a estrutura organizacional da equipe de TI da Uni Piaget CV?
2. Quantos servidores possuem a instituição?
3. Quem são as entidades que utilizam os recursos de TI?
4. Como são divididos os computadores, domínios (estacão de trabalhos) entre laboratórios e departamentos da rede?
5. A instituição utiliza ERP, sistemas académicos, base de dados? Quais?
6. Como é feita a comunicação entre unidades? Utilizam VPN para troca de informações de forma segura?
7. Mais mecanismos são utilizados para mitigar os riscos? (firewall etc…..)
8. Cada Campus possui a sua equipa de TIC?
9. Desenvolvem, adquirem e mantêm as aplicações para garantir a segurança?
10. Existe alguma política de segurança sendo utilizada?
11. Como é feita a manutenção dos computadores, servidores?

12. Caso não exista uma PSI implementada, quais dos seguintes itens abaixo, interessa no desenvolvimento de uma PSI para a Uni Piaget que abrangesse a realidade actual da instituição?

Segurança Lógica

(x) Utilização de Rede (x) Administração de Contas

(x) Utilização de E-mail (x) acesso de internet

(x) Uso de Impressoras (x) Uso de estacão de trabalhos

(x) Vírus e códigos maliciosos (x) uso de Notebook/dispositivos móveis

( ) utilização de softwares (x) Uso de Intranet

( ) acesso remoto (x) Senhas

(x) Backups ( ) outros que acharem pertinentes

Outros:

Segurança Física

(x) Controle de acesso (x) Mesa Limpa e Blq. De Ecrã

(x) Utilização de laboratórios de Inf. e salas de projecção

( ) outros que acharem pertinentes

Outros:

Segurança dos RH

(x) Continuidade de negócios "disponibilizar contactos da equipa de segurança"

(x) social "cair na Eng. Social" ( ) outros que acharem pertinentes

Outros: